UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	No. 2:11-cr-00070-RAJ
	)	
	)	
vs.	)	Seattle, WA
	)	
ROMAN V. SELEZNEV,	)	
	)	Jury Trial, Day 3
Defendant.	)	August 17, 2016

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE JUDGE RICHARD A. JONES
UNITED STATES DISTRICT COURT

APPEARANCES:

FOR THE PLAINTIFF:

NORMAN McINTOSH BARBOSA
U.S. Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
norman.barbosa@usdoj.gov

C. SETH WILKINSON
U.S. Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
seth.wilkinson@usdoj.gov

HAROLD W. CHUN
U.S. Department of Justice
1301 New York Avenue NW, Suite 600
Washington, DC 20005
harold.chun@usdoj.gov

FOR THE DEFENDANT: JOHN HENRY BROWNE
Law Office of John Henry Browne
108 South Washington Street, Suite 200
Seattle, WA 98104
johnhenry@jhblawyer.com

EMMA SCANLAN
Law Office of John Henry Browne
108 South Washington Street, Suite 200
Seattle, WA 98104
emma@jhblawyer.com

Andrea Ramirez, CRR, RPR
Official Court Reporter
United States District Court
Western District of Washington
700 Stewart Street, Suite 17205
Seattle, WA 98101
andrea_ramirez@wawd.uscourts.gov

Reported by stenotype, transcribed by computer

I N D E X

E X H I B I T S

THE CLERK: We are resuming our jury trial in the matter of the United States vs. Roman Seleznev, Cause Number CR11-70, assigned to this court.

DAVID DUNN, having been previously sworn, was examined and testified as follows:

THE COURT: Counsel, you may continue your direct examination.

MR. BARBOSA: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. BARBOSA

Q Good morning, Detective Dunn.

A Good morning.

Q Yesterday you went over quite a bit of information in a fairly rapid fashion. I'd like to show you two exhibits, including one that was just admitted towards the end of the day. I have on the screen here 6.10A and 6.2.

First, with reference to 6.2, can you remind the jurors what this exhibit included?

A These are logon IP addresses that -- they were provided by Yahoo! for access to the rubensamvelich@yahoo e-mail account.

Q And then 6.10A, in the left side?

A Is the confirmation e-mail from WebNames.ru for the registration of the domain name track2.name. And that e-mail was sent to rubensamvelich@yahoo.com.

Q Can you -- using the diagram to the left of the big board,

17.7 --

MR. BARBOSA: And if the witness may step down from the stand?

THE COURT: He may.

BY MR. BARBOSA

Q Can you explain for the jurors how these two exhibits tie in with the diagram there in front of you?

A So ultimately, the e-mail accounts -- this e-mail account was used to register the track2.name e-mail account. This e-mail account was also accessed from this server. So this server was -- this server was being used to read these e-mails, and then the registration was also sent to that account.

Q Okay. Go ahead and take your seat again.

Did you also find e-mails in the rubensamvelich account related to e-currency sites?

A Yes.

Q Can you explain what an e-currency site is?

A Sure. So there are a number of digital currencies that exist on the internet. They are not controlled by any nation. They're not backed by a national bank. And they've been created to allow the online transfer of money between two entities. And so they're commonly used in the underground economy for people to move money anonymously. There's no way to subpoena records from them. They don't follow typical banking regulations, like, know your customer, or any of those

type of rules or regulations.
Q Has law enforcement pursued some of these online currencies?
A Yes.
Q Does one of those include Liberty Reserve?
A Yes.
Q Did you find any e-mails in the rubensamvelich account related to Liberty Reserve?
A Yes.
Q Can you refresh the jury's understanding of exactly what Liberty Reserve is?
A So Liberty Reserve is one of those online currency exchange companies where people can hold money in deposit. So you can have money in your Liberty Reserve account, just like you would with a standard bank. Or you can transfer between your Liberty Reserve account and somebody else's. So if I owed you money for something, I could directly transfer from my Liberty Reserve account to another Liberty Reserve account.
Q In your review of the track2 or bulba sites, did you find any indications that those sites were accepting Liberty Reserve as a payment form?
A Yes.
Q How would they accept Liberty Reserve as a payment form?
A So through the bulba website, one of the ways to fund your account was to make a direct Liberty Reserve or WebMoney

transfer to the Liberty Reserve account for bulba.cc.

Q Do you have the binder with Exhibit 6.15, so 6.15?

A Yes, I do.

Q Can you review that exhibit?

A Okay.

Q That exhibit is a total of six pages; is that right?

A That's correct.

Q Without going into the specifics of what the content of those e-mails is, what is the nature of those e-mails?

A The -- regarding the registration and use of a Liberty Reserve account.

Q Are you familiar with how one would go about registering a Liberty Reserve account?

A Yes.

Q What happens when you register a Liberty Reserve account?

A So you would go to the Liberty Reserve website. You would register for an account. You can provide -- the information you provide doesn't have to be factual. So it's just like signing up for one of many online type of accounts. There are a few additional security measures. You receive a unique PIN number to access the site. And then once you have that, you have the ability to then fund your account.

Q Does Liberty Reserve send out any kind of automatic confirmations of creation of account?

A Yes. Once you've created the account, they send you an

e-mail telling you you need to log in to activate the account.
Q In your experience, are those e-mails generated by a human, sitting at a computer?
A No. They're automatically generated by the system at Liberty Reserve.
Q How do you know that?
A Because I've received -- I've registered a Liberty Reserve account myself.
Q Does Liberty Reserve also monitor -- did it have the types of velocity controls that you had discussed earlier on, in terms of fraud detection?
A Yes.
Q What types of velocity controls did you see Liberty Reserve using?
A Geolocation for IP addresses.
Q How would they use that?
A They would look at what your most recently used IP address was, and where it was geographically located. And if they saw a difference in the next IP address that was significant, they would alert you to the fact that they saw that discrepancy, in the event that it's potentially fraud.
Q Are you -- based on your training and experience, both in the private sector and in law enforcement, are you familiar with how those types of velocity control notices are generated and sent to a user?

A Yes.
Q How are they generated and sent to a user?
A They're automatically generated.
MR. BARBOSA: The government offers Exhibit 6.15.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 6.15 was admitted)
BY MR. BARBOSA
Q Turning to the first page of Exhibit 6.15, what is this notice here?
A So this is the notice of a successful Liberty Reserve account registration for Liberty Reserve Account Number U0045772.
Q And what was the sending address for that e-mail?
A No_reply@libertyreserve.com.
Q Based on your training and experience, what does that tell you about how that e-mail was generated?
A Automatically.
Q So is this the account confirmation e-mail that you just referenced?
A That's correct.
Q And have you received e-mails like this from Liberty Reserve?
A Yes.
Q Turning to Page 2, what is this e-mail?

A This is an e-mail notifying the e-mail account that they had observed the account being accessed from a different IP address location; and that they've sent a verification PIN, and he needs to log into his account to verify.

Q When was that?

A May 28, 2010.

Q What was the IP address that Liberty Reserve had recorded in their systems?

A 66.36.240.69.

Q And where do you see that on Exhibit --

A That's the HopOne server, located in McLean, Virginia.

Q Turning to Page 3, does the same IP address show up again?

A Yes.

Q And when was that dated?

A June 7, 2010.

Q Page 4, this is another IP address. This is a different one; is that correct?

A This is a different IP address for a server also located at the HopOne facility in McLean, Virginia.

Q Is Page 4 the main HopOne server that you have listed on Exhibit 17.7 again?

A That's correct.

Q Sorry. That was Page 5 that I was looking at.

And then finally, Page 6, does that have the .69 number again?

A Yes, it does.
Q Excuse me. I think I'm getting a cold.
All right. Moving on to Exhibit 6.19, can you look at that in the binder in front of you?
A Okay.
Q That's two pages; is that correct?
A That's correct.
Q What is the nature of these e-mails, without going into the content?
A It's in relation to making a payment from a Liberty Reserve account to another company.
Q And who sends the e-mail on the first page of Exhibit 6.19?
A The e-mail account rubensamvelich@yahoo.com.
Q And does that contain other statements from the user of the rubensamvelich account?
A Yes.
MR. BARBOSA: Government offers Exhibit 6.19.
THE COURT: Any objection?
MS. SCANLAN: Your Honor, as to Page 1 of 6.19, if it's offered not for the truth of the matter asserted as to the e-mail from invest@approvedinvest.com, then the defense has no objection.
MR. BARBOSA: That's correct, Your Honor. The e-mail from invest@approvedinvest.com is only offered to show context

to the writer's response.

THE COURT: All right. Ladies and gentlemen of the jury, you've heard the exchange of counsel. It's not offered for the truth, only to provide context, and that's how you should treat this particular exhibit. Otherwise, 6.19 is admitted.

(Exhibit 6.19 was admitted)

BY MR. BARBOSA

Q Turning your attention to the top of Page 1 of Exhibit 6.19, what did the user of the rubensamvelich account state?

A "It's not my account. I didn't enter it. My account is U9614915. I never use any other accounts. Please pay my money."

Q What was the message that he was responding to?

A He was responding to -- do you want me to read it?

Q Summarize it.

A Basically, they were telling him that his Liberty Reserve account was incorrect, and they provided a different Liberty Reserve account number.

Q So they had the wrong number.

A Yes.

Q And his response?

A This is what my number is, and it's the only one I've used.

Q Turning back to 6.15, so do you have two different accounts that the user of the rubensamvelich e-mail account had identified as belonging to him?
A Yes.
Q Did the user of the rubensamvelich account also send a message indicating what his username was?
A Yes. "My username is smaus1."
Q Was that the same username we've gone over before?
A Yes.
Q Did you find any e-mails in the account related specifically to communications with the nicknames "track2" or "bulba?"
A Yes.
Q I'd like to have you look at Exhibits 6.20 and 6.21, in the binders in front of you. Each of those is a one-page exhibit.
Do you recognize those?
A Yes.
Q How do you recognize those?
A These are e-mails that were sent to rubensamvelich@yahoo.com.
MR. BARBOSA: Government offers Exhibits 6.20 and 6.21.
MS. SCANLAN: The defense has no objection to Exhibit 6.21. We have a hearsay objection to Exhibit 6.20.

THE COURT: Counsel for the government?

MR. BARBOSA: Your Honor, a question is not hearsay, under Rule 801. And 6.20 is a question and a request.

MS. SCANLAN: The first sentence is not a question. It's a statement.

MR. BARBOSA: And it's also a statement of a co-conspirator.

THE COURT: The objection is overruled. 6.20 and 6.21 are admitted.

(Exhibits 6.20 and 6.21 were admitted)

BY MR. BARBOSA

Q Can you go over this for the jurors?

A This is from the email account andreid.ca@gmail.com to rubensamvelich@yahoo.com, with a subject of "track2 register." The e-mail specifically states, "I want a track2.name account. Do you know where shall I go and register? CVV only." And there's a date, 2010-10-2, and then it's signed "andreid.ca."

Q Is track2.name one of the websites on your chart, 17.7?

A Yes.

Q What -- based on your training and experience in carding investigations, what does "CVV only" mean?

A So there are two primary types of credit card fraud. The first is to purchase the full credit card track data, which has the full card number with the separator and all of the additional discretionary data. That's the information that you

would use to conduct in-person fraud. You would recode that on a counterfeit card and use that for in-person fraud. "CVV only" means you just want that 16-digit account number, the expiration date, and the card verification value, which is that three-digit number on the back. And that would be used for online or telephone-related fraud. Those are the identifiers you need to make an online purchase. So this person wants that second type of card to purchase.

Q Turning to Exhibit 6.21, what do we have here?

A This is an e-mail generated by ICQ. The subject is "ICQ account confirmation." It says, "Hi track2.name," space, "bulba.cc. Thanks for joining ICQ. Click here to complete your ICQ registration. If the link is broken, simply copy and paste the following URL into your browser," which I won't read the whole URL. "Thanks, the ICQ team. Need help? Visit our frequently-asked questions page."

Q So I'd like to go back to what was previously admitted as Exhibit 16.10.

Can you explain, again, what ICQ is?

A ICQ is an internet chat program that at the time was run by AOL. And it's -- within ICQ, each user is assigned a unique number, which they can identify themselves with. They can also assign a nickname to it, if they want. So you can have a number, as well as be known as "track2," "bulbacc," and you can communicate with each other.

Q So in Exhibit 16.10, when you were going over the information -- the forensic chat that you found on the Cleveland drive, was that an ICQ conversation?
A Yes, it was.
Q Had you seen the name "bulba" show up elsewhere in the rubensamvelich account? Was this the only place it showed up?
A It was, I believe, in one other place.
Q The rubensamvelich account, what was it primarily linked to?
A The track2.name.
Q I'd like to show you Exhibit 6.16 now, which is 15 pages. Tell me if you recognize those.
A Yes.
Q How do you recognize these e-mails? What's the nature of these e-mails, without discussing the content?
A Sure. So these are messages from carder.su, which is a well-known carding forum, that were sent to track2.
Q And how are -- why are messages from a carding forum forwarded to or sent to an e-mail account?
A So when you create an account at carder.su, you fill in your account registration information. That includes the nickname you want to use, you give, you know, a password, and then you would also provide an e-mail. If somebody wants to send you a private message, once that private message is sent, the carder.su system would then e-mail you, telling you that

you had a message and go check it. So this is just informing him that he had a private message within the carder.su platform.

Q And who are these e-mails addressed to?

A They're addressed to track2.

MR. BARBOSA: Government offers Exhibit 6.16.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: 6.16 is admitted.

(Exhibit 6.16 was admitted)

BY MR. BARBOSA

Q We'll go through some of these e-mails for the jurors, starting with Page 1.

Explain -- have you seen messages like this before?

A Yes.

Q You discussed a little bit about how they're created.

Can you go over this first message, on Page 1?

A Sure. So this is a private message. And it's to track2. "Dear track2: You have received a new private message at carder.su - All about network security from FreshShop, entitled 'FreshShop.net Admin.' This message that was sent, 'Hello: I need a favor, brother. I'm admin of freshshop.net. Recently closed my site. I'm working on script development services now, and shop design. But few months ago, I logged into the account ccplus. It was friend's account. It is not me. But

because I logged into the account, they think I'm a clone. Can you please drop the claim on the ccplus account? Just post saying 'claim dropped.'"

Q What would a "claim" be on carder.su?

A So on the forums there are strict rules about who can do what. And one of the big things that they try to prevent people from doing is having multiple accounts. They don't want somebody to set up a new card shop and then log in as a separate user and talk about how great that card shop is, because you're basically promoting your own product; so they try to keep the duplicate accounts to a minimum.

So in this case, it appears that track2 had made a claim that they -- he had seen two different accounts logging in by the same person. And this guy was trying to explain the back story, to try to get that claim dropped, so he could access his account.

Q Is that based on your experience reviewing the carder website?

A Reviewing this carding website, taking down other carding websites, yes.

Q Turning to Page 2, what was the message that track2 received from carder.su here?

A The message was, "Before I contact you ICQ, need AMX," which is American Express, "with CVN/AVS. Do you have?"

So again, like we had talked about earlier with the card

verification value, this is somebody who wants AmEx numbers that can be used for online fraud.

Q Turning to Page 3, what was the subject of this e-mail?

A Again, another private message. And this is from user "mOrda." "Hi. Can I get membership for your shop somehow? Thanks."

Q Page 4?

A This is a message from yury.kindrat. And the message was, "Hi. I want to register on your site. Could you help me with that?"

Q Did you see any of track2's responses to these private messages in the rubensamvelich account?

A No.

Q Why not?

A Because to respond to these, he would have logged into the carder.su portal and responded from there. So his responses would have been sent to the e-mail addresses of the other users.

Q So where would you have to go to find those?

A You would have to either try and seize the carder.su server, or you would have to go to the e-mail accounts belonging to those other users.

Q Looking at Page 5, can you go over this e-mail for the jurors?

A This is from a user by the name of "Theftmaster." "Hi,

tr2. I asked a while back about maybe reselling for you. You send me ICQ and said get in touch. I was sick a while, so I never got in touch. What ICQ are you on? Maybe you could run true terms with me, see if it's doable or not. You know I'm about since the CP days," which is another carding forum called CarderPlanet, "with script" -- script is another well-known carder -- "and those guys, so I probably know you from way back as we all change nics. Hope to talk soon."

Q Let's break that down a little bit.

Based on your training and experience, what does "reselling" mean?

A He basically wants to buy card numbers in bulk from track2 and resell them.

Q Okay. And moving towards the end, based on your training and experience, this comment, "We all change nics."

A This guy is basically saying, you may not know me as theftmaster. You may know me as a previous nickname, because I've previously changed my nic.

Q You've mentioned a couple times your ability to identify some of the IP addresses, that HopOne address.

Did you find any other e-mails related to these servers, specifically to HopOne servers, in the rubensamvelich account?

A Yes.

Q Showing you what's been marked as Government's Exhibit 6.11, which is three pages --

MR. BROWNE: Sorry. What was that again?

MR. BARBOSA: 6.11.

MR. BROWNE: Thank you.

BY MR. BARBOSA

Q Do you recognize that?

A Yes.

MR. BARBOSA: Government offers Exhibit 6.11.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 6.11 was admitted)

BY MR. BARBOSA

Q What do we have here in Exhibit 6.11? What are these e-mails?

A This is the activation e-mail that was sent to rubensamvelich from admin@robobill.net, which includes the IP address, domain login and password credentials, and control panel credentials for a server located at 66.235.184.36.

Q Is there a second server listed also?

A It's actually a second IP address for the same server, which was 66.235.185.80.

Q How could there be two IP addresses on a single server?

A For backup, dual honing on the server. Just gives you -- if one IP goes down, or is saturated, you have a second link to get in.

Q And can one physical computer server be used to host multiple servers, multiple server programs or server operating systems?
A Yes.
Q Turning to Page 2 of that exhibit, you see some of the IP addresses that you've come across before?
A Yes.
Q Which ones have you come across before in the rubensamvelich account or elsewhere?
A So this is the activation for another service at IP address 66.36.228.124, also 66.36.250.190.
Q And finally, turning to Page 3, did you find the IP address that was the main HopOne server that you focused on?
A Yes, this is the activation e-mail for 66.36.240.69 and 66.36.246.158.
Q When did these e-mails come in? Did they all come in on the same day?
A No, they didn't come in on the same day. They started January 30, 2010, for the first one; March 4, 2010, for the second two.
Q Now turning your attention to Exhibit 6.22, do you recognize this e-mail?
A Yes.
Q How do you recognize Exhibit 6.22?
A This is a response from rubensamvelich@yahoo.com to

abuse@robodesk.biz, related to an abuse complaint that he'd received on his server.

Q Turning you, before we go over the content of this, to Page 19 of that exhibit, did this indicate whether or not this was an automated message that he had received and responded to?

A Yes.

Q What -- okay.

A Specifically -- do you want me to read it?

Q Just the notice.

A "Note this is an automated e-mail response to the incoming scan/attack."

MR. BARBOSA: Government offers Exhibit 6.22.

THE COURT: Any objection?

MS. SCANLAN: Your Honor, the objection is only to Pages 20 through 25, which are not automated messages, as far as I can tell.

THE COURT: And Counsel, the top part of 21, is your objection to the entirety of that page, or just the bottom half?

MS. SCANLAN: That's correct, Your Honor, just the bottom half.

THE COURT: And Counsel, 25, the same question, because it appears --

MS. SCANLAN: Same answer, Your Honor.

THE COURT: All right. Let me hear from the

government.

MR. BARBOSA: Your Honor, the statements of the other side, the other side of this conversation, are only offered for context for the responses from the author, the rubensamvelich account, which are party opponent statements. And therefore, I believe they come in to offer context to the responses.

THE COURT: The objection is overruled. They'll be admitted.

(Exhibit 6.22 was admitted)

THE COURT: Members of the jury, again, as it relates to Page 20 through 25 -- actually, the entirety of this exhibit -- it's only offered for purposes of context, not for the truth of the response. So if the communication comes from Romper Stomper, then that's admissible as substantive evidence. But if it's not from Romper Stomper, you should only consider it for purposes of context. Otherwise, they're admitted.

Please proceed.

BY MR. BARBOSA

Q Detective Dunn, what was the nature of the e-mail string in Exhibit 6.22?

A That the IP address 66.235.184.36 had been engaging in scanning of Port 3389. And abuse@robodesk.biz had received complaints about that scanning and were notifying the rubensamvelich e-mail account. And then there was a discussion where rubensamvelich states, "I cleaned the virus last time.

Now it's active again. Don't know how. Can you please reformat the server? Because I can't clean it. Thanks you."

Q How are abuse complaints like this generated? What is the purpose of these?

A The purpose of these is to notify the server owner that something malicious is occurring on their server, so that they're aware of it and can take steps to fix it.

Q This particular server, the IP address identified, where was that at?

A It was at the HopOne data center in McLean, Virginia.

Q Was that one of the three that the rubensamvelich account had received a receipt for?

A Yes.

Q Three or four.

Going to Page 2, what information does the automated abuse complaint produce?

A It produces the source IP address. It gives you the protocol. So it was a TCP type of connection. And then it gives the destination address that was scanned. So these are just sequential in order, showing that an entire range was scanned for Port 3389.

Q And in your training and experience, are you familiar with these types of automated reports?

A Yes.

Q Can you explain for the jurors -- you used a lot of

technical terms there -- what this shows you?
A This shows me that somebody using the server at 66.235.184.36 launched a scan of a large number of IP addresses within that range of the 213.133 network segment, and was just scanning all these servers to see if any of them would communicate on Port 3389, to see if they would accept a remote desktop connection.
MR. BARBOSA: Your Honor, may the witness step down to the exhibit?
THE COURT: He may.
BY MR. BARBOSA
Q Based on your training and experience, can you explain for the jurors how this fits in on the diagram on Exhibit 17.7?
A Sure. So there were -- we're going to call this laptop up here the suspect -- the suspicious computer that we've been referencing now. So this device is scanning just large swaths of the internet, looking for Port 3389, to see if it's willing to accept a connection.
Q Again, what is Port 3389?
A That's the remote desktop port. So then as it relates to the rest of the case, if it were to find Port 3389, it would then launch a dictionary attack against that to see if it could properly guess the username and password. And if it did, then it would gain access to the victim machine. In this case, hopefully, it would be a point-of-sale system with credit card

numbers.

Q Okay. The computer, the suspect computer in the upper left-hand corner, would that have the IP address that it launched the attack?

A Yeah. This is the computer that's launching the attack. So there was a server at HopOne that was launching the attack, yes.

Q But the HopOne is in the lower right-hand corner.

A Well, this is one of the HopOne servers. So this is the HopOne server ending in "69." So this is another -- the way I explain it, I just refer to this as another HopOne server that was launching the attack.

Q I see. Now, again, based on your training and experience, would somebody be physically sitting at the HopOne server in Virginia to launch this attack, with a laptop like --

A No. Somebody would have been logged in from anywhere in the world. And then they would have remoted in to the HopOne server. And they would have had their tools on that HopOne server, allowing them to do these large-scale scans. They would have set it up to do the scan, launched it. It would have taken some time. And then once the scan was done, they would get a report back saying, I scanned these however many tens of thousands of IP addresses, and here's the list of five or ten or a hundred that are willing to accept that remote desktop connection. And then they would continue their

activities from there.
Q You can go ahead and take your seat again, then.
THE COURT: Counsel, let's let the jurors take a stretch break.
Members of the jury, if you'd like to stand?
Please be seated. Counsel, you may continue.
BY MR. BARBOSA
Q Based on your training and experience, did you form an opinion regarding how the HopOne servers might relate to your investigation?
A Yes.
Q What was that opinion?
A That they were being used to scan for potential new victims that could be hacked into. And they were also being used to collect stolen credit card information.
Q Did you form any opinion as to how they might be used in relation to the e-mail accounts?
A That they were also being used to access the e-mail account.
Q So turning your attention to approximately December 2010, did the HopOne -- did any of the HopOne IP addresses come up in relation to another computer intrusion event?
A Yes.
Q What was the nature of that report?
A We received a report of a business in the Washington, D.C.

area that had been hacked into. And they had located a version of the malware, similar to what we had previously seen, that was now sending stolen card data to the 66.36.240.69 IP address, if I have that correct, off the top of my head.

Q Going back to your first victim, Schlotzky's Deli, was that sending data to the HopOne center?

A No.

Q Where was that sending data?

A It was sending data to a server in Russia.

Q Based on your training and experience, why would a hacker use a server in the United States?

A There are a number of reasons why you would use a server in the United States. Number one is cost. Servers in the U.S. tend to be cheaper, in general. Number two, a U.S. IP address is trusted more than a Russian IP address, especially when your victim is located in the U.S. That's a less suspicious connection, if somebody were to go through your computer and say: Okay, who are you talking to? Why are you talking to Russia?

So when I went out to Schlotzky's, I immediately honed in on the kameo malware that was running, because I thought to myself, "Why would a deli in Coeur d'Alene, Idaho, have a connection to Russia?" It made no sense to me. That was how I initially got suspicious of that process. So you take that out of the equation by having it report back to a server in the

U.S.

The U.S. power grid is more reliable, so your server is going to be less likely to go down. The McLean, Virginia, area is the largest concentration of fiberoptic cables in the world --

MS. SCANLAN: Objection. Narrative.

THE WITNESS: -- so you have very fast internet connections there. There's a lot of reasons.

THE COURT: Let's go one at a time. The objection is to narrative.

MS. SCANLAN: Yes.

THE COURT: Objection is overruled. The witness is still answering the question.

You may continue with your response.

THE WITNESS: So there's a lot of fiberoptic cables there, so you have a very fast and reliable internet connection in the HopOne area.

BY MR. BARBOSA

Q What did you do first in regards to these HopOne server IPs when you discovered this connection?

A We obtained a trap-and-trace order for internet connections going in and out of the servers.

Q Can you explain what a "trap-and-trace order" is?

A So a trap-and-trace order allows us to just look at the IP addresses that are communicating with the server. We don't get

the content, so we don't know what they're saying back and forth. We just know that IP Address 1 contacted the HopOne server, and IP Address 2 contacted the HopOne server. So it gives us an idea of how much communication is going back and forth between the servers.

Q Is this like a wire tap?

A It's not a wire tap. A wire tap gets you content. So a wire tap on a phone would get you the actual call. You would hear the calls. Or on a computer, you would see what the e-mails were. This is more of a -- you would see just -- for phone numbers, you would just see which phone number called the other phone number. You wouldn't know what the call was about.

Q How do you go about obtaining a trap-and-trace order?

A So we obtained a 2703(d) court order.

Q What do you mean "2703(d)"?

A It's a court order signed by a judge that allows us to install a device to capture that connection information.

Q So what type of information -- connection information does a trap-and-trace order get you, when placed on a server?

A So it tells us what -- the two IP addresses that were communicating with each other. It tells us the protocol that they were communicating on. And the -- and that's about it, and the dates and times that the communications occurred.

Q What did the HopOne trap-and-trace order record in relation to connections with the HopOne servers?

A That there were large numbers of connections going back to the HopOne server, specifically on Port 80. So --
Q What is Port 80?
A Port 80 is the internet port, and also the port that stolen credit card numbers were transmitted on from their malware.
Q So bringing you back to what was admitted already as Exhibit 1.1, and I want to draw your attention to the command line you showed us for the kameo and shmak malware, this HTTP.
What would that communicate over?
A Port 80.
Q Okay. Where were these connections coming from?
A They were coming from primarily all over the United States.
Q And did it tell you the type of data that was being transmitted?
A No.
Q Just the address?
A Correct.
Q Were these records helpful to your investigation?
A Yes.
Q How were they helpful to your investigation?
A With some of the IP addresses, we were immediately able to identify businesses that were communicating. Some of the businesses actually had the IP addresses registered directly to

them. So there were a number, particularly one in the Maine area, that we were able to identify immediately as a likely compromised business, because their IP address was registered directly to them.

Q Let me slow you down, because this is probably out of a lot of people's expertise.

What does that mean, the domain address -- or excuse me -- the IP address was registered directly to them?

A So most IP addresses, like our home IP addresses, are registered to Comcast, right, or CenturyLink or Verizon or whoever we use. For many small businesses, that is also the case. For some medium-size and larger businesses, the IP addresses are registered directly to them. So, for example, Nordstrom's would probably have IP addresses that are directly registered to Nordstrom's. In this case, we found an IP address for a business in Maine that was directly registered to that retail business.

Q Did you do anything with that information?

A Yes.

Q What did you do?

A We contacted the Secret Service office in Maine and asked them to contact that business and explain that we suspected that they were infected with malware.

Q Did you obtain a forensic image of their computer system?

A Yes.

Q Did you review it?
A Yes.
Q What did you find?
A That they were infected with the -- with a version of the malware from this case.
Q And did it have any references to the HopOne servers?
A Yes.
Q What were those references?
A Specifically, that the server coded into that malware was designed to transmit to the HopOne server.
Q And what was it designed to transmit to the HopOne server?
A Credit card numbers.
Q Did you find -- well, I'll go back to that later.

So some of these IP addresses, you said, you were able to identify directly. How did you go about identifying the IP addresses that weren't directly registered to the business?
A We sent subpoenas out to the internet service providers to ask them who their customers were.
Q What did you learn about these IP addresses? What type -- who was the user of these IP addresses that you were seeing on the trap-and-trace order?
A They were, for the most part, small businesses located throughout the U.S., a lot of pizza shops, a lot of fast-food restaurants, small retail stores.
Q That process of requesting subscriber records through

subpoenas, was that efficient and effective for you? Were you able to identify all the IP addresses?

A It was not efficient, but it was effective. It took, you know, several weeks to get all those returns back. But we were able to identify the majority of the victims.

Q You said the majority. Did you learn of any other method to narrow your focus and make it easier to identify the IP addresses that you were seeing on the HopOne trap-and-trace order?

A Yes.

Q What was that?

A We did two things. Number one, we identified one vendor that was specifically impacted, and we subpoenaed all of his records. And then we eventually got a search warrant for the HopOne server.

Q Let's go back to that vendor. What was that vendor?

A There was a company called Granbury Restaurant Technologies.

Q And how were they related to this investigation?

A We noticed that a large number of pizza shops were -- had been hacked into and were reporting to the HopOne server. We identified that they had a specific point-of-sale software called Firefly, which was written by Granbury Restaurant Technologies. So we contacted Granbury and were able to determine that those systems all had a common username and

password.
Q So how did this -- how did your contact with Granbury help you go about identifying more of the businesses that were behind these IP addresses?
A Because they provided us with records of their clients and the IP addresses that they knew belonged to their clients.
Q Showing you what's been marked as Government's Exhibit 15.1, which is 17 pages long, do you recognize that?
A Yes.
Q How do you recognize that?
A This is the list of customers that had been provided to us by Granbury Restaurant Technologies.
Q And does that identify their customers with their IP address?
A Yes.
MR. BARBOSA: Government offers 15.1, pursuant to a 902 certification.
THE COURT: Objection?
MS. SCANLAN: Yes, Your Honor.
May we have a sidebar, please?
THE COURT: As it relates to 15.1?
MS. SCANLAN: Yes, Your Honor.
(The following proceedings were heard at sidebar)
MS. SCANLAN: We got a list at 8:00 a.m. this morning of the exhibits the government was going to use today. I'm

trying to --

MR. BARBOSA: Did I not include that?

MS. SCANLAN: Well, I'm trying to go through this, but this one is not on it. We do have -- I do have an objection to this exhibit in terms of this witness laying the foundation for what appears to be this customer list. My greater concern, also, is that we have additional objections to some of the other exhibits that are going to come in this morning, that I wasn't aware were coming in until we just started all this.

THE COURT: Why don't we take a break now, have the jury be excused, and just deal with it at one time.

(End of proceedings heard at sidebar)

THE COURT: Members of the jury, it's going to take a little bit longer than I expected, so we're going to take a short recess. So please proceed back to the jury room.

(Jury exits the courtroom)

THE COURT: Do we need to have the witness excused?

MS. SCANLAN: I have no objection to the witness remaining.

MR. BARBOSA: He may be helpful.

THE WITNESS: Can I use the restroom and come back?

THE COURT: Sure.

One thing, before we get started, Counsel, the Court's observed a few things that have developed, as we've progressed

with the trial. And I know at the beginning of trial there was exchange of interpreters providing interpreter services for Mr. Seleznev. And then I started noticing that he didn't have the headset on. And then today I notice that there's no translation being provided by one of the interpreters.

We're continuing to make them available, so is this on an as-needed basis, or what's the defense position?

MS. SCANLAN: May I have a moment to speak with my client?

THE COURT: Sure.

(Off the record)

MS. SCANLAN: As-needed would be helpful.

THE COURT: Well, let me ask you this, Counsel. We have two interpreters here. And it's not that we can't continue to have them available, but I'm not sure if it's a waste of court resources to have two interpreters here, full time, for the balance of the two weeks, if it's on an as-needed basis.

So let me hear from you, after you want to consult with the interpreters. Because I don't know what kind of volume of need is going to be necessary for the defendant.

Is there any way that you can assess, Counsel, when there would be a greater likelihood that your client would need more interpreter services?

MS. SCANLAN: My prediction of that would be that the

level would remain constant from this -- what we're observing right now.

THE COURT: I don't understand what you mean, Counsel.

MS. SCANLAN: What I mean is that I don't think the need is going to increase or decrease, based on the remainder of the evidence that's coming in.

THE COURT: All right. Do you see that changing for any particular witness, or series of witnesses, or categories of witnesses?

MS. SCANLAN: I don't. This is highly technical. So I don't think it's going to get more -- slightly more technical than this, maybe, which may require slightly more interpreting.

What I've observed is actually there's more interpretive services needed when it's more dialogue, as opposed to this type of evidence. So perhaps he may need more help with some of the alleged victim witnesses, the business owners, who are just going to be talking conversationally. But I agree with Ms. Noble, the interpreter, that she can probably provide that service as needed, individually, without two interpreters.

THE COURT: Okay. I'll tell you what, from the government's perspective, what's the order of witnesses who are going to testify? In other words, how long do you think Mr. Dunn is going to go?

MR. BARBOSA: I think Mr. Dunn will testify through

the remainder of today, possibly into cross on tomorrow morning. We have additional law enforcement witnesses for the remainder of the week, which will be a lot of technical testimony, also. We expect to begin calling victims on Monday. And we will have FDIC and NCUA witnesses on Friday for a fairly short testimony, banking related.

THE COURT: Let me ask you this, will the interpreters be available on an on-call basis? In other words, at the end of the day, counsel could identify the witnesses that they believe they'll be calling the following day. And then if you believe, Counsel, based upon that, we need an interpreter, that we could have two, as opposed to one. Is that workable? Because I don't want to tie the interpreters up, that they would be prevented from working someplace else.

INTERPRETER: Your Honor --

THE COURT: If you'd use the microphone, please.

INTERPRETER: -- this interpreter can be available for the entirety, because we essentially blocked out the three weeks.

I think it's possible that somebody could be on call, but it's -- you know, if it meant preventing them from accepting other work, that would probably be some kind of a hardship, and I don't know how the Court would handle that, necessarily. So I can't really speak for my colleague as to whether or not she can remain available indefinitely, or whether it would just be

kind of hit-and-miss. I mean --

MS. SCANLAN: May I have one moment?

THE COURT: Sure.

MS. SCANLAN: Your Honor, I think that the collective opinion of the interpreters and the defense is that we only need one interpreter, and we do not need a second interpreter on call.

THE COURT: Okay. Then we'll proceed in that fashion. I'll let the interpreter stay until the lunch hour, if you'd like, and then we can separate at that point in time.

Now, so the defense is accepting to having just one interpreter, Counsel?

MS. SCANLAN: Yes, Your Honor.

THE COURT: I want to make sure Mr. Seleznev has a full opportunity to have full translation. I'm not trying to minimize or curtail that in any way. But it was just an observation, that we go from the jury seeing the defendant with two interpreters; and then all of a sudden, there's none. And I don't want to create the impression that he's not interested in knowing what's going on. Because at this point in time, based upon the government's opening statement, they see an individual who they don't believe is from the United States, may not even speak the language. So I'm trying to make sure that there's the appearance of fairness all the way around.

So if there's no objection, we'll cut it down to just one

interpreter. And if anything changes, where Mr. Seleznev believes that he needs to have the benefit of full-volume, full interpretation services, we'll activate two again, Counsel.

MS. SCANLAN: Thank you, Your Honor.

MR. BARBOSA: Your Honor, I think in light of this development, a full record that Mr. Seleznev sufficiently understands what's going on, and that this was his choice, is necessary. I think confirmation from Mr. Seleznev, that he does understand sufficiently, may be appropriate.

THE COURT: Counsel, are you representing on behalf of your client that he understands sufficiently?

MS. SCANLAN: Speaking on behalf of my client, we would object to an inquiry of our client regarding his understanding of the English language in this case.

THE COURT: I think that's been an issue in terms of what he understands and what he doesn't understand, particularly, for example, when he was contacted in the Maldives, and the statement that he made about the passport. There may be question whether or not he understood what was being said to him. And I don't want to give the impression to the jury that he does or does not understand the English language, based upon any decisions that I've made.

So I'm not going to inquire of Mr. Seleznev. I'll trust counsel as an officer of the court. She's been in communication with her client. As an officer of the court, she

represents to the Court that there is a sufficient understanding for a conscious decision that he's made to choose not to have two interpreters, and not to have active interpretation, only on an as-needed basis.

Is that a fair summary, Counsel?

MS. SCANLAN: Yes, Your Honor.

THE COURT: Now, Counsel, let me hear your objection.

MS. SCANLAN: I think -- the Court brought up the witness order. The other issue that came up right before we started this morning, which is going to relate to why we're here right now, is the idea that Agent Mills is going to come and testify next. He was not on the witness list from the government for this week. They gave us a list of everyone for this week, which is very helpful, but Agent Mills was not on that list, and he's now being substituted in. And I understand that's because of travel arrangements. That makes sense. But we are not prepared for him to take the stand today.

THE COURT: Mills?

MS. SCANLAN: Yes.

THE COURT: Well, Counsel has indicated he's not going to testify today, and that Dunn may go into tomorrow, particularly cross examination.

MR. BARBOSA: Let me explain. I think it's highly unlikely he will. I think that Detective Dunn, based on the pace we've set so far, especially as we don't even have the

jury right now, it's very unlikely Detective Dunn will finish today. If it somehow very rapidly sped up and we finished, Agent Mills would be the only witness we have available to begin testifying today.

MS. SCANLAN: That's my concern. Agent Mills is a -- obviously, he's the case agent. He's been here all day. His testimony is very important. And learning at 9:00 a.m. that he may come on the stand today, I'm not adequately prepared to have him testifying today.

THE COURT: When did counsel give you the list of witnesses expected to testify either today or this week?

MS. SCANLAN: When did they give me that list? They gave me that list last week, but Agent Mills isn't on it.

THE COURT: His name is not on the list at all.

MS. SCANLAN: Correct. It's on their overall witness list, but not on the list of witnesses for this week.

THE COURT: All right. Well, let's do this, Counsel. We don't know if Detective Dunn is going to finish, so we could spin around this for the next 20 minutes. I'm not going to do that. What I am going to do is hear your objections. We'll deal with Mills, if he does come up and testify, at that time.

MS. SCANLAN: Okay. So I do have an objection to this witness laying the foundation for Exhibit 15.1, which is the Firefly customer list.

THE COURT: Your specific objection?

MS. SCANLAN: I don't think he has sufficient knowledge to know that this list is kept as a business record by this company for these specific businesses.

THE COURT: Okay. And your objection to the other exhibits, Counsel?

MS. SCANLAN: So the other exhibits, as I understand it -- I've been through the exhibits that were identified this morning. The other exhibit that I think has a lengthier objection is Exhibit 5.3.

THE COURT: Let me catch up.

Okay. I'm with you, Counsel, 5.3.

MS. SCANLAN: And the translation, Your Honor, is at 5.3A. So it's not the images themselves. It's the message they're attached to, which is translated at 5.3A.

THE COURT: I'm at 5.3A, Counsel.

MS. SCANLAN: I'm sorry, Your Honor?

THE COURT: I'm at 5.3A. So what's your objection?

MS. SCANLAN: The objection is that this is hearsay, and it's not for context, and it's not a co-conspirator. And it is essentially -- it's offered from this person to show the identity of this e-mail account holder. And I don't think there's an exception under the hearsay rule for this information.

THE COURT: Okay.

MS. SCANLAN: And I'm done talking about that.

THE COURT: I didn't know if you had another one, Counsel.

MS. SCANLAN: Your Honor, right now, that's the only one I have. I'm trying to be as efficient as possible with these.

THE COURT: I appreciate that.

MS. SCANLAN: But it's hard to listen to the witness and go through the exhibits at the same time, which is what we're doing.

THE COURT: I understand.

Let me hear from counsel for the government, first on 15.1.

MR. BARBOSA: Thank you, Your Honor.

Let me bring that up on the overhead.

THE COURT: I have it in front of me.

MR. BARBOSA: So 15.1 is a business record from Granbury Restaurant Solutions. And we discussed this as part of the pretrial conference. 15.1 had a 902 certification that the Court has already ruled was sufficient authentication. This comes in under Rule 902, and the Court has already addressed that as part of the pretrial hearing, that it was sufficient. Detective Dunn does not have to establish a business records foundation for it. I think that's all for 15.1.

In terms of 5.3A, we addressed in our trial brief, and

more recently in our submission about evidence found in an e-mail account, how this type of evidence should come in, because it connects defendant to a crime scene. It is circumstantial evidence of defendant's dominion and control of these e-mail accounts. And I believe this comes in under the case law that was cited in our trial brief and our recent submission. This is a photograph of defendant -- excuse me -- defendant's ex-wife and their daughter. And the comments in the translation state, "Greets her daddy. Chewing hand, daddy," and, "What a fashionable binky." It clearly connects the defendant to the boookscafe account, which is one of the crime scenes in this case.

THE COURT: Counsel, I'm going to reserve on that. Over the recess, I'll look at 5.3 and look at what you provided in your brief. I'm not going to make a ruling without having a chance to refresh my memory about what was provided.

And Counsel, did you provide a response briefing to that particular objection?

MS. SCANLAN: To be honest, Your Honor, I don't actually remember, right off the top of my head, whether we responded to that particular item.

THE COURT: Okay. Nor do I. That's the reason I want to look at it over the break.

MS. SCANLAN: Go ahead.

MR. BARBOSA: And I just want to clarify, my

understanding is that counsel does not have an objection to 5.3, is that correct, the untranslated exhibit?

MS. SCANLAN: Well, the objection would remain the same, whether it's in Russian or English, as to the first -- and I did have a question -- that's what I was about to say -- before we get into the weeds on this, since we're here right now, regarding whether the government intends to have a witness identify the people in these photos, like Detective Dunn, for instance.

MR. BARBOSA: Yes.

MS. SCANLAN: Okay. So I do have an objection to Detective Dunn identifying, at the very least, the baby, who I'm pretty sure he has never seen before. I don't know if Detective Dunn has personally met with Svetlana. That's possible.

MR. BARBOSA: He has.

MS. SCANLAN: So the objection would remain as to the child.

THE COURT: All right. Counsel?

MR. BARBOSA: I did not intend to have him identify the child.

THE COURT: Okay. That eliminates that concern, Counsel.

MS. SCANLAN: Okay.

THE COURT: All right. Counsel, as to 15.1, that

objection is overruled. Upon offering in front of the jury, 15.1 will be admitted.

As to 15.3, the Court reserves ruling until I've had a chance to look at that over the break or recess.

MR. BARBOSA: And that was 5.3, Your Honor.

THE COURT: 5.3, excuse me.

MR. BARBOSA: As well as 5.3A.

THE COURT: Both of them, Counsel.

MR. BARBOSA: And for the Court's information, our case law regarding the receipts is at Page 4 on our request for ruling on the opening slides.

THE COURT: What's the docket number, Counsel?

MR. BARBOSA: It's going to be one of the last ones that was submitted -- I apologize. I only have a copy that's printed up without the docket number.

THE COURT: I know I have it in my trial notebook, Counsel. I just wanted to see if you had the docket number. So if it's one of the last ones, we'll pull it up.

Anything else before we bring the jury in?

MR. BARBOSA: No. Thank you, Your Honor.

MS. SCANLAN: No, Your Honor.

MR. BROWNE: Are we having a break, or not?

THE COURT: Not until 10:30.

MR. BROWNE: Thank you.

(Jury enters the courtroom)

THE COURT: Good morning, ladies and gentlemen of the jury. Please be seated.

Counsel, you may continue your direct examination.

MR. BARBOSA: Thank you, Your Honor.

BY MR. BARBOSA

Q When we broke, Detective Dunn, you were discussing how you went about identifying the businesses that -- behind the IP addresses you found in the HopOne trap-and-trace. The government is just -- the Court has just admitted Exhibit 15.1.

Can you explain for the jurors what this is and how you use this?

A Sure. These are records that were provided by Granbury Restaurant Technologies for their lists of customers that utilize the Firefly point-of-sale system. The list included the business name and address, as well as the IP address that Granbury had on file for that business. I compared the IP list from this with the data from the trap-and-trace to see if the data correlated.

Q Did the data correlate with any of these companies?

A In total, approximately 25 percent of these businesses had been compromised.

Q So this list that Granbury provided of all of their customers, were every one of these customers on the HopOne server?

A No.

Q So not all of these had been breached.
A Correct.
Q What was the percentage, you said?
A About 25 percent.
Q Okay. What did you do after identifying some of the businesses that were on the HopOne trap-and-trace?
A We did a number of things. We sent agents out to some of the businesses to collect forensic images from those businesses. We contacted all of the businesses that were located in the state of Washington. And we sent victim notification letters to the rest.
Q Did you examine computer images from many of those victim businesses?
A Yes, I did.
Q What did you find, in general, when you were examining those systems?
A I found a consistent pattern of those businesses being accessed remotely. I found a version of the kameo malware family on those victim business computers. I found communications with the HopOne server. I found internet history that was consistent with the downloading and installation of the malware from the FVDS server in Russia.
Q You've -- let's go back to the HopOne -- well, actually -- sorry.
Can you step down for a moment, with the Court's

permission? You just referenced the FVDS server, and I'd like you to point out where that is.

A This server right here (indicating).

Q How did you find that on the victim computer images?

A So when I did a forensic examination on the victim computer images, what I found was that once they had been compromised, the hacker would open up a web browser. And in his web browser, he would type in a URL, which would either be shmak.fvds.ru or smaus.fvds.ru. And then he would put a forward slash, and he would type the name of the malware that he wanted to download. So if he wanted to download kameo, he would type in kameo.exe. If he wanted to download the next version, which was called dtc2, he would download dct2.exe. If he wanted to download the next version, which reported to HopOne, he would type in dtc4.exe. And that would download the malware from this server onto the victim system so he could then install it. So that was how this server fit into the whole picture.

Q And where was that malware coming from, geographically?

A Russia.

Q And then going back to the other side of the chart, the HopOne server.

A Right. This server was also used, at one point, as a collection server --

MS. SCANLAN: Objection, Your Honor. Nonresponsive.

THE COURT: Ask another question, Counsel.

BY MR. BARBOSA

Q Was the shmak server used for any other purposes?

A It was also used to collect stolen card numbers from one of the malware versions.

Q Now I'd like to draw your attention to the right side bottom of the chart, the HopOne server.

You've shown us three or more IP addresses that you've identified as HopOne. Why is the 66.36.240.69 number the only one listed on this chart?

A It was the server that was primarily used as part of the infrastructure. So this server collected the stolen card numbers. It was the only server at HopOne that actually received stolen card numbers. It was also the server that was used for some internet activity.

Q Let's -- can you take the witness stand again?

A Yes.

Q After you began identifying the businesses behind these IP addresses that you saw connecting to the HopOne server and confirmed the malware on their systems, what did you do next?

A We obtained a search warrant for the HopOne servers.

Q When was that, approximately?

A January 19, 2011.

Q Who obtained the search warrant?

A Agent Wojcieszek, in the Eastern District of Virginia.

Q Is that where the servers were located, physically?
A That's correct.
Q Why did -- did you go out for that search?
A I did not.
Q Who seized them?
A Special Agent Leopard and Special Agent Wojcieszek.
Q Did they physically seize the servers?
A They seized the hard drives from the servers.
Q What did they do with the drives' servers?
A They took the drives to the Secret Service cyber forensic lab at Secret Service headquarters, in Washington, D.C., and created forensic images from those drives.
Q Did you receive a copy of the forensic images?
A Yes, I did.
Q And were you able to confirm the integrity of the forensic images using the same methods you described earlier in your testimony?
A Yes. I verified the hash values.
Q Did you examine the HopOne servers?
A Yes.
Q Using the same methods to examine as you described earlier?
A That's correct.
Q In general overview terms, before we start using exhibits, could you explain what you found on the HopOne servers?

A I found several hundred victim businesses that were transmitting approximately 180,000 stolen credit card numbers to that server. I found information related to plane tickets that were purchased using the server. I found malware associated with the case on the server. I found hacking and scanning tools on the server.

Q Did you review the internet history on the servers?

A Yes.

Q Did you find anything in the internet history?

A Yes.

Q What types of things did you find?

A I found web browsing. I found plane ticket reservations in certain names.

Q You said you found approximately 180,000 credit card numbers on the servers.

A That's correct.

Q How were they stored on the servers?

A They were stored in log files. And so there would be a log file, and the log file would have a name. And the name of the file was an IP address.

Q And what were those -- were you able to identify those IP addresses?

A Yeah. Each IP address belonged to a different business.

Q As you went about identifying those businesses, did you find any businesses in the state of Washington?

A Yes.
Q Specifically, in Western Washington?
A Yes.
Q Do you recall the names of some of those businesses?
A Casa Mia Italian Restaurant in Yelm, MAD Pizza on Thomas Street in Seattle, MAD Pizza on Madison Street and First Hill in Seattle, MAD Pizza in Madison Park, Village Pizza in Anacortes, MAD Pizza located in Tukwila.
Q How were those servers configured to be used?
A They were point-of-sale systems.
Q I'm sorry. Going back to the HopOne servers.
How were the HopOne servers configured to be used?
A The HopOne server was running an Apache web server, so it was -- along with PHP. So it had a web server to collect the data from the malware set up.
Q What is "PHP"?
A PHP is a type of computer code.
Q And you said it was running an Apache web server.
What is an Apache web server?
A Apache web server is an open source, or free, web server, that somebody can install. And it allows for the server to communicate and host content. So it's an enterprise server type application.
Q I'm bringing up Exhibit 1.1 from the Schlotzky's exam, and turning your attention again to the HTTP code, how does that

relate to an Apache server, or the PHP that you just discussed?
A So the malware, in this case, was designed to send the stolen card numbers to IP address 188.120.225.66.
Q And where is that on 17?
A That's in Russia.
Q Is that the shmak server?
A Yes. Specifically at that server to send it to a PHP file called ftm.php. So that file is waiting there on the web server to collect the data. And then that file would then address that data, once it got to the server.
Q So this malware on Schlotzky's system, would it have sent anything to the HopOne server?
A No.
Q Okay. If a victim was configured to send to the HopOne server, what would you see on their system?
A You would have seen the malware version dtc4.exe, which was configured to send to the 66.36.240.69 IP address.
Q Did you find anything like that during the course of your examination of victim computer systems?
A Yes.
Q Could the HopOne servers -- well, actually, let me ask you this.

Did you review logs related to how the person administering the servers logged in?
A Yes.

Q What types of logs did you review?
A I reviewed the system event logs.
Q Why do you review system event logs?
A They show remote desktop connections into the system.
Q What types of logs do you review?
A The system event, application, and security event logs.
Q Are those three separate logs?
A Yes.
Q Let's go over the security event logs.
What do those show you?
A Any security-related incidents associated with the computer.
Q Do they tell you if the computer had been remotely accessed?
A Yes.
Q Okay. You mentioned application logs; is that correct?
A Uh-huh.
Q What do you review those for?
A Those show you logs related to any programs that are installed on the system.
Q And network logs?
A System event logs was the third one.
Q Sorry, system event logs.
A Those are for system-process-related logs.
Q What types of things do you review those for?

A Base Microsoft operating system events.
Q Do any of these tell you what username was used to log into the system?
A Yes.
Q Which log tells you that?
A The security event log.
Q Were you able to determine where the user was connecting from?
A Yes.
Q How?
A Along with the login information, it shows the IP address from where that login is being initiated.
Q And where were those coming from?
A Primarily Bali, Indonesia, and some from Russia.
Q Showing you Exhibit 3.31, which is ten pages, do you recognize this?
A Yes.
Q As part of preparing for trial, did you focus on logins to the HopOne server from Indonesia?
A Yes.
Q Is this an exhibit of those logins?
A Yes.
MR. BARBOSA: Government offers Exhibit 3.31.
MS. SCANLAN: No objection.
THE COURT: Admitted.

(Exhibit 3.31 was admitted)

BY MR. BARBOSA

Q What do we see here?

A These are logins and logouts for the username "shmak" onto the 66.36.240.69 server at HopOne. So then we have a list of IP addresses that were used.

Q And these are incoming IP addresses to HopOne?

A Yes.

Q And what user is logging in from these IP addresses?

A The Windows user account named "shmak."

Q And had you seen that word "shmak" before on any of the infrastructure?

A Yes.

Q Where?

A "Shmak" was used as one of the malware names at one point.

Q And did you see it on other servers?

A Yes.

Q Which ones were those?

A It was located on another server at HopOne.

Q How did you determine where these IP addresses were located geographically?

A I did a Whois Lookup on the IP address.

Q And where did they come back to?

A The Bali, Denpasar, Indonesia area, for these ones.

Q Turning your attention to what was previously admitted as

Exhibit 15.5, what was previously admitted for demonstrative purposes as 15.2, the excerpt of 15 -- let me start completely over.

Referring you to Exhibit 15.2A, a demonstrative, which is an excerpt of Exhibit 15.2, were there any connections to Bali, Indonesia, or parts of Indonesia, in this exhibit, from Western Union?

A Yes. Roman Seleznev was picking up Western Union wire transfers in Sanur and Denpasar, Indonesia.

Q Have you reviewed the passport that was seized from Mr. Seleznev at the time of his arrest?

A Yes.

Q Did you see any indications in there that he had been traveling to Indonesia in the time period covered by the login records for the HopOne server?

A Yes.

Q What did you see?

A That he traveled to Bali, Indonesia.

Q How often did he travel to Bali, Indonesia, based on your review of the passport?

A Very frequently.

Q You described how the HopOne server was maintaining the credit card numbers that you found in log files.

Did you pull, as exhibits, some examples of those log files?

A Yes.
Q And did you find any lists indicating the totality of, like, all of the log files?
A Yes.
Q Showing you what's been marked as Government's Exhibit 3.1, do you recognize this?
A Yes.
Q This is a seven-page exhibit.
How do you recognize this?
A This is a list of the active log files that were collecting card numbers on the server.
Q Does that fairly and accurately capture the list of active log files?
A Yes.
MR. BARBOSA: The government offers Exhibit 6.1 -- sorry -- 3.1.
MS. SCANLAN: No objection to 3.1.
THE COURT: 3.1 is admitted.
(Exhibit 3.1 was admitted)
BY MR. BARBOSA
Q You said this was a list of active log files.
Are you distinguishing that from something else?
A Yes.
Q What?
A There were -- in addition to the active log files that

were collecting on the server at the time that we seized it, there were other sets of log files that had -- were no longer collecting card numbers and had been moved to a different location on the drive.

Q So focusing in on the first line, or first entry, on Exhibit 3.1, what information is included here in this exhibit?

A So it's the name of the log file, which has -- is the name of the IP address that it collected it from; the date that the log file was first created; the last time anything was written to that log file; and then the full file path for the log file.

Q What does the file path tell you?

A It shows me where on the drive exactly that log file was located.

Q And which one of the HopOne servers were these log files located on?

A 66.36.240.69, the primary one, that's on the diagram.

Q What is -- what is the importance of the "file created" and the "last written" dates here?

A It shows when the -- this new file began to be written, so the first time a card number was written to the file, and then the last time a card number was written. And then in between cards were being written.

Q Based on your training and experience and examination, have you formed an opinion on whether this was the only time cards were being written for this particular victim?

A This was not the only time, no.
Q Why do you believe that?
A There were three different sets of log files for most of the victims. Each set of log files lasted approximately two weeks.
Q And did you form an opinion as to how these log files were being used by whoever was operating the HopOne server?
A Yes.
Q What was your opinion on that?
A That the log files would be allowed to collect card numbers for a period of time, a week and a half to two weeks. The log files would then be collected, the stolen card numbers extracted from those log files and placed up for sale, and then basically reset, and new log files would then be written to collect cards again, let it run for a couple of weeks, harvest them, and start a third time.
Q You -- focusing in on the "last written" date, you indicated that you obtained your search warrant on January 19.

How does this date, this last written of 1/20/11, relate to when the search warrant was executed?
A That was when the search warrant was executed, on the 20th.
Q Why isn't the "last access" date in here?
A Because the last access date isn't applicable to when the last card was written to the file.

THE COURT: Counsel, we're a little bit past 10:30. Is this a good time to take a morning recess?

Members of the jury, we'll take our morning recess at this time.

(Jury exits the courtroom)

THE COURT: Anything we need to take up, counsel for the government?

MR. BARBOSA: No. But the docket number was 404, if you haven't found that.

THE COURT: Anything to take up, Counsel?

MR. BROWNE: I don't believe so.

(Recess)

THE COURT: Counsel, I wanted to revisit the question on the admissibility of 5.3 -- all right. I want to revisit the question of 5.3 and 5.3A. Counsel for the defense has indicated there's no difference between the two exhibits as far as the nature of the objection.

The Court has looked at the briefing that was supplied by counsel for the government. There's no briefing that was provided by the defense on this specific point, so the Court has to look to case authority that was provided. The specific case I'm looking at is the Ninth Circuit opinion. It's *United States vs. Huguez*, H-U-G-U-E-Z, hyphen, *Ibarra*, I-B-A-R-R-A.

And that case cross references an issue regarding the admissibility of notepads. And the objection was that the

Court had erred in admitting notepads, because the government didn't sufficiently identify -- or sufficiently establish the factual predicate for their admission as co-conspirator statements. They argue, then, under *State v. Ordonez*, O-R-D-O-N-E-Z, 737 F.2d. 793, which is also the Ninth Circuit, 1984, that the government was required to lay a foundation for admission of drug ledgers. *Ordonez*, however, held only that the hearsay rule prohibits the introduction of drug ledgers without a foundation when the ledgers are being admitted to prove the truth of the matters asserted in them.

In this case, the trial judge made clear in his limiting instructions to the jury that the ledgers were not being admitted to prove the truth of what was written in them. Instead, they were admitted to show that the type of activities charged in the indictment were being carried out in the residence. It also goes on to note, thus, the rule against hearsay was not implicated, and the requirement of a proper foundational showing for admitting the records to prove the truth of the matters asserted was not triggered.

So when reading that opinion, the conclusion the Court comes to is that with the proper instruction to the jury, that the exhibit is not being offered to prove the truth of the matter, in other words, the communications that took place, but rather it's limited to show the type of activities charged in the indictment that connect the user of the account.

So the Court sees, in 3.3A, which I can read, because that's in English, that makes reference to communications such as how she's greeting her daddy, showing daddy what a fashionable binky, things like that. The communications aren't being offered to establish the identity or relationship between Mr. Seleznev and his child or his spouse. It's offered to demonstrate or show the use of the books -- B-O-O-O-K-S-C-A-F-E, @yahoo.com account. So that's the same as the residence in the case that the Court provided to the parties. So in lieu of a residence, we have the bookstore account.

So I think under those circumstances, the hearsay claim of contention by the defense is not activated, but the Court will instruct the jury that 5.3 and 5.3A are admitted for the limited purpose of showing that the type of activities charged in the indictment connect the user of the -- are being offered to show the connection to the bookstore account, and not for anything else.

Anything further for counsel for the government or the defense?

MR. BARBOSA: No, Your Honor.

MS. SCANLAN: Your Honor, I'm sorry, in terms of the limiting -- the instruction the Court proposes to give to the jury --

THE COURT: Yes.

MS. SCANLAN: -- what activities -- I just missed whatever portion of -- the activities in the e-mail are admitted for what purpose?

THE COURT: In other words, the government, I believe, was offering these e-mails, 5.3A and 5.3, as it relates to the use of the boookscafe account. And it's not the content of the communications that the exhibit is being offered. It's to show the connection of the use of the boookscafe to the user. And I believe that's the only purpose.

Is that what the government's represented?

MR. BARBOSA: Correct.

THE COURT: All right. That's the only limited purpose for which these can be used.

You still have a question on your face, Counsel. You're not saying anything.

MS. SCANLAN: I'm trying. To the user, meaning the user of the e-mail account?

THE COURT: User of the boookscafe@yahoo.com account.

MS. SCANLAN: Okay. I guess my only confusion is that -- my understanding is that they're offering the pictures, and Detective Dunn is going to testify that that is Mr. Seleznev's wife. That's offered for that fact.

THE COURT: All right. Counsel for the government?

MR. BARBOSA: The witness is certainly allowed to identify somebody he recognizes in a photograph. He will not

identify, I believe, the child, because he has not met the child. But he has, in fact, met Svetlana Selezneva, so he can identify her in the picture.

THE COURT: But then that gets back to the content of the communication. Is it then being offered for the truth?

MR. BARBOSA: No. Because the content of the communication is not what he's identifying her based on. He's identifying her based on the photograph, which is unquestionably not hearsay. It's a photograph. And it's in the account. He can identify somebody in a photograph.

THE COURT: Let me ask you this, do you even need the content of the communication, other than the fact of the use of the booookscafe@yahoo.com?

MR. BARBOSA: Yes. Because once he has identified the person in the photograph, the presence of the name "Svetlana" is the name that connects the account to the defendant. That's the hearsay exception that we've essentially briefed. It's the connection between somebody who is identified, not from the content of the e-mail, but from the photograph that was attached. And then it ties up that loop and connects the defendant to the account.

MS. SCANLAN: Are we talking about the briefing regarding the HopOne server airplane ticket, in Docket 404? I just want to make sure I understand what's being referenced.

MR. BARBOSA: Yes.

THE COURT: I'm referring to the government's brief that's the government's request for a ruling on objections to opening statement slides.

MS. SCANLAN: Okay. Regarding the airline ticket?

THE COURT: No. I'm looking at Page 4, Counsel.

MS. SCANLAN: Thank you, Your Honor. I think we are looking at the same thing. I just want to make sure --

THE COURT: It's the material from the HopOne server, on Page 3?

MS. SCANLAN: Yes. I just wanted to make sure I wasn't missing briefing on this actual e-mail.

I don't really -- I think that the content of the e-mail, in terms of the written content, is being offered, as the government seems to be saying, for the truth of what is in the content, to go with the truth of what's in the picture.

THE COURT: Any further argument from the government?

MR. BARBOSA: No. I think you have it exactly right. It is circumstantial evidence connecting the defendant to the account. It doesn't become relevant until the witness can actually identify the person in the photograph, and then that brings the entire thing full circle.

THE COURT: All right. The Court will admit the exhibit. I'll provide a limiting instruction. We can bring the jury in now.

(Exhibits 5.3 and 5.3A were admitted)

(Jury enters the courtroom)

THE COURT: Good morning, again. Please be seated.

Counsel, we're going to come back to "3" after lunch. I want to spend a little more time on this.

Please continue.

BY MR. BARBOSA

Q When we broke, Detective Dunn, you were talking about the list of log files. And you mentioned -- the exhibit we were going over, 3.1, was the active log files.

How many other log files were there?

A There were several hundred other log files, and they were in two other separate groups.

Q What were the two other separate groups; do you recall the names?

A They were -- I don't recall the names of the groups. They were date ranges.

Q And where did you find the other lists of log files?

A In the recycle bin.

Q Were those written at different dates?

A Yes.

Q Were you able to determine the total number of -- sorry.

Let me ask this. What was in the log files?

A Additional stolen credit card numbers.

Q Were you able to determine the total number of stolen credit card numbers that were recorded in these log files?

A Yes.
Q How many?
A Approximately 180,000.
Q Did you do anything with those 180,000 credit card numbers to try and determine if they had been used for fraudulent purchases?
A Yes.
Q What did you do?
A Provided them to the card brands, as well as certain financial institutions.
Q What did you ask the card brands and the financial institutions for?
A To provide me with any loss information related to those cards.
Q Why did you ask the credit card brands to provide you with information about losses on the cards?
A The credit card brands collect and retain records as it relates to losses on cards, so they would be the best source to go to for that information.
Q What type of information can the card brands provide you when you send them credit card numbers to research?
A They can look at their records and determine dates, location, merchant ID numbers, and transaction amounts for credit card transactions that had been deemed as fraudulent.
Q Are you familiar with how the card brands receive and

maintain records of unauthorized charges on individual cards?
A Yes.
Q How did you become familiar with this?
A Through extensive contact with the card brands, through working with a financial technology firm, through my work in law enforcement in fraud investigations.
Q You mentioned working with a financial technology firm. Was that your private-sector employment?
A Yes.
Q How do the card brands collect this type of information?
A That information gets reported to them through their network by either the merchant acquiring bank or the issuing bank.
Q What is the difference between a merchant acquiring bank and an issuing bank?
A So during any credit card transaction, there are two banks that are involved. There's the issuing bank, which is the bank that issues you your credit card. So if you have a Bank of Americard [sic] in your wallet, that's the issuing bank. And then there's the merchant acquiring bank, which is the bank that processes the credit card on behalf of the merchant. So the store that you go into, it's their bank. And then they communicate to each other through the card brands network. So they would communicate through the Visa, MasterCard, American Express, or Discover network.

Q Why do the banks report this information to the card brands, this information about unauthorized charges?
A Because the mechanism for refunding the charges goes back through the card brands, as well. And then the card brands also collect the information so that they can identify trends in credit card fraud, identify additional common points of purchase. It's just standard business records so they can combat fraud.
Q Are the banks required to report this information to the card brands, as part of their relationship with them?
A Yes.
Q What type of information do the card brands receive from the banks related to unauthorized charges in particular accounts?
A They receive the date and time of the transaction, the amount of the transaction, whether or not the transaction was authorized or not, the merchant identification numbers, merchant addresses, a lot of information.
Q Do they receive these records from the banks at or near the time the unauthorized charges are recorded?
A It's when the unauthorized charges are reported.
Q So at or near the time?
A Yes.
Q Is that fairly immediate?
A Yes.

Q Do the card brands investigate the loss reports to ensure their accuracy?
A Yes.
Q How do they go about investigating them?
A Working with the financial institutions. They also work with the merchant acquiring processors to determine if there is a breach location to send out private forensic investigations. Quite a number of steps are taken.
Q And do they keep these records in the ordinary course of their day-to-day business?
A Yes.
Q Is making these records something they do only for law enforcement?
A No.
Q Would they maintain these records even if you weren't going about asking them for them, as law enforcement?
A Yes.
Q Why do they maintain this type of information?
A There's statutory requirements to retain that type of information. The information is of value to them to help combat fraud. Their clients request the information.
Q What do you do -- when you receive loss information back from the card brands, what do you do with that information you receive back from them?
A When I receive loss information, I provide it to an

analyst within Secret Service to review.
Q And what is the analyst's task?
A To deduplicate any loss that's in there, to identify the institutions that were impacted, to come up with a total loss value, just to analyze that information.
Q You said "deduplicate information." Why would there be duplication?
A In some cases, we would receive -- from some of the large institutions, they would send us fraud directly related to the cards. And then the card brands would send us that same information. So we would make sure that we don't have the same information twice.
Q Did you also provide the card brands with the names of the victim businesses?
A Yes.
Q Did that produce additional information?
A Yes.
Q Were those -- were the records related to the victims, specifically? Did they always tie directly back to a credit card number you found in your investigation?
A No.
Q So how would -- why would they provide you information on credit cards that you hadn't found, for example, on the HopOne server?
A Because I asked them for all the fraud associated with the

merchants that I gave them a list of.
Q As your investigation continued, did you send additional credit card numbers beyond the ones you found on the HopOne server?
A Yes.
Q Where were the sources of your credit card numbers that you provided to the card brands?
A A security researcher had provided me with some additional card brands.
Q And where were those from?
A A server in the Ukraine.
Q Is that another collection server that you've identified?
A Correct.
Q Did you obtain some numbers directly from the forensic images of the victim systems?
A Yes.
Q Which victims were those?
A The Broadway Grill.
Q Just that one?
A That was the primary one, yes.
Q So let's go back to the HopOne server. Did you -- you testified earlier about the process of identifying the victims based on their IPs that you found on the HopOne server.
Did you create a summary to list out all of the identifying victims that you've tied back to a server?

A Yes.
Q Showing you what's been marked as Exhibit 16.12, do you recognize this?
A Yes.
Q And this is a 16-page exhibit. How do you recognize that?
A This is a spreadsheet that I created to show the IP address, the victim information, as well as whether or not I had found full credit card track data in the log files associated with that victim.
Q When you discussed the Granbury list of customers, you said only approximately 25 percent of those customers were, in fact, victims, had actually been breached.
Is this list different in that regard?
A Yes.
Q How is this list different?
A Every one of these victims had some form of the malware on it.
Q And are these victims that you'd seen on the collection servers?
A Yes.
Q Were you able to identify every single one of them? Were there some that you couldn't find an identifying information for?
A Yes.
Q Approximately how many of those, in percentage-wise?

A Maybe 10 or 15 percent.

MR. BARBOSA: Government offers Exhibit 16.12 as a summary exhibit.

MS. SCANLAN: May I inquire?

THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Good afternoon. Can you hear me?

A Yes.

Q Good morning, excuse me. Good morning.

Are you saying that for each of these businesses that's listed under "customer name," in Column C, that you have actually verified that each one of these has the malware installed on it?

A I have not been to each one of these, no.

Q Okay. Let me make sure I understand that, because I thought that's what you just said.

So each one of these businesses is connected to the IP addresses you found on HopOne; is that what you're saying?

A Yes.

Q But you don't know whether each one of these businesses was infected by the malware issued.

A No. I know that each one of these businesses was sending stolen card data to the HopOne server.

Q Okay. And so is that -- that's the unifying theme for all

these, is that they were sending things to HopOne?
A Yes.
Q And did you verify that information with these individual businesses, or just from the server?
A Based on the server records. And some of them we verified it with. We sent out -- we imaged about 20 servers, in total. And then some of these were also -- had private forensic investigations done, as well.
Q But some of these, when you went there to identify them, there was no indication that they had the transmissions from their server to the HopOne server; correct?
A There's not a single one on here that I went to that I didn't find malware. So everybody that I went to had malware.
Q And I'm sorry, what percentage of these did you go to?
A I think I went to seven, total.
Q And there is how many, total?
A Several hundred. And then Granbury also remotely accessed a large number of them and found malware, as well.
Q Okay. But you have not verified -- you verified seven of the 519?
A Yes.
Q So as far as -- just so I understand, so this is a compilation that you made of businesses and IP addresses found on the HopOne server.
A Yes.

Q And seven of those, you have verified with that business's server that it was sending information to HopOne.
A Seven that I personally went out to, and then there's another ten or so that I have additional images from that I verified, as well; so about 20 that I verified personally.
Q Okay. So that's 20 of the 519?
A That I verified personally, yes.
MS. SCANLAN: With that information, I have no objection.
THE COURT: 16.12 is admitted.
(Exhibit 16.12 was admitted)
DIRECT EXAMINATION
BY MR. BARBOSA
Q So is there any legitimate reason these businesses would be sending their credit card numbers to the HopOne server?
A No.
Q And to be clear, this has how many different IP addresses on it?
A 519.
Q Each one of these had a log file on the dump collection servers?
A Yes.
MS. SCANLAN: Objection. Leading.
THE COURT: It is leading, Counsel.
////

BY MR. BARBOSA

Q What does each one of these IP addresses represent?

A A log file that was found on the servers.

Q And let's go over this chart, starting at the top. You have several columns. We've gone over what the IP address is.

What does Column B indicate?

A Whether or not I personally viewed full track data in the log file.

Q And where would you view that full track data?

A From the log files from the servers.

Q Turning down to Line 25, or IP 24.105.183.226, this doesn't have full track data.

What does that indicate?

A I just typed in "Track 1" and "Track 2," meaning that I saw both tracks there.

Q But not full track data?

A That is full track data. I just, for whatever reason, typed that in.

Q Variation?

A Four years ago.

Q Were there some that had no track data in the log files on HopOne?

A Yes.

Q For example, Line 36?

A Yes.

Q And Line 56?
A Yes.
Q How many approximately -- what was the percentage, approximately, that did have full track data in the log files on the collection server?
A Eighty-five to 90 percent.
Q And what were the primary businesses that you identified that had been breached?
A Pizza restaurants.
Q Were there a smattering of other businesses?
A Yes.
Q Any particular types?
A There were a number of garden centers. There were zoos and aquariums. Those are the primary other business types.
Q Where were these businesses located, primarily, geographically?
A Primarily in North America. Most of them were in the United States.
Q Did they cover many of the states?
A Yes.
Q How many victims, approximately, did you identify in the state of Washington?
A Victim businesses?
Q Yes.
A Eight.

Q If you don't have that offhand, that's fine.
A Eight.
Q I'm sorry?
A Eight.
Q Eight. Okay. Out of how many?
A 519.
Q As part of your examination, did you pull the contents of the underlying log files that are listed in Exhibit 3.1 and the other log files you found in the recycle bin?
A Yes.
Q I'm showing you what's been marked as Exhibit 3.2.
Do you recognize this?
A Yes.
Q What is this exhibit?
A This is the contents of the log file for Log Number 207.155.207.163.
Q Does that fairly and accurately capture the content of that file?
A Yes.
Q And where did you find that?
A That was on the HopOne server.
MR. BARBOSA: Government offers Exhibit 3.2.
MS. SCANLAN: No objection.
THE COURT: 3.2 is admitted.
(Exhibit 3.2 was admitted)

BY MR. BARBOSA

Q So we're looking at Page 1, which we've blown up the top portion of this.

What do we have here?

A This is the contents of what had been transmitted to that server from the IP address. And it includes stolen credit card information.

Q And is that -- where is the stolen credit card information?

A In the dark -- I'm looking for a dark number.

Which exhibit number is this?

Q Sorry, 3.2. The data I've focused in on, underneath the full path.

A Okay. So we can see just over to where -- to the right of your cursor, you see "438." That's a card number right there. There's another one. Five lines up, there's a card number. There's one kind of lower, lower, to the left. Right there, yep. There's a track. There's one at the very bottom row right there.

Q These card numbers that we've explained, unfortunately, publicly, are these still active card numbers, based on your training and experience?

A 7/13, six of 12 -- no. They're all expired.

Q And as part of your process of informing the card brands of these numbers, did they go about canceling these cards?

A They notified the financial institutions and gave them an opportunity to cancel.
Q Okay. And these are over six years old; is that right?
A Yes.
Q So we have an IP address here that -- what is that? Is that the name of the file?
A That is the name of the file.
Q Using Exhibit 16.12, can you identify that particular IP address? And then I'll read it back to you.
A Line 13.
Q Line 13?
A Yes.
Q Where is that from?
A That's from the MAD Pizza at 14800 Starfire Way, in Tukwila, Washington.
Q Is that one of the victim businesses that you responded to and actually examined their machines?
A Detective Hanson responded and collected the image, and then I examined it.
Q And going back to the top of Exhibit 3.2, what does this tell you about when this data was being sent from MAD Pizza Starfire to HopOne?
A From January 10, 2011, at 11:47 a.m., until January 19, 2011, at 22:19 hours.
Q Based on your training and experience, does that represent

the only credit card numbers that were being transmitted from MAD Pizza Starfire?

A No.

Q Why not?

A Because there were two other log files.

Q Did you find additional log files from them?

A Yes.

Q When you examined their system, did you find additional -- did you find malware on their system dating prior to this January 10, 2011?

A Yes.

Q Did you pull a similar log file for Village Pizza?

A Yes.

Q Showing you what's been marked as Exhibit 3.3, do you recognize this?

A Yes.

Q How do you recognize it?

A The log file for Village Pizza.

MR. BARBOSA: Government offers Exhibit 3.3.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 3.3 was admitted)

BY MR. BARBOSA

Q Okay. I've zoomed in on the top of Exhibit 3.3.

What do we have here?
A So this is just showing what the log file was, and that its name was 71.121.225.225. And it was created January 10, 2011, and last written on January 19, 2011.
Q And the full path name, what information comes from your examination computer versus from the original image?
A So I named the case "HopOne servers track2." So that was from me. "Disk image" is the name of the -- that it was a disk image. Then it starts at "C," so the "C" drive. And then the rest of it is the path on the drive, so "server\SERVER\home\non-existent-host\logs.
Q And which HopOne server did this come off of?
A 66.36.240.69.
Q And again, turning to 16.12, I'm going to move down to Line 107.
Do you see that IP address on this list?
A Yes.
Q And what was it?
A Line 107 is for Village Pizza.
Q Where were they located?
A 807 Commercial Avenue, Anacortes, Washington.
Q How many pages of credit card numbers were found in the log file for Village Pizza?
A Off the top of my head, I don't remember.
Q I'm showing you Page 29 of the exhibit.

Is that the end of the log file?
A Yes.
Q And the MAD Pizza exhibit that we went over for page -- in Exhibit 3.2, three pages of data?
A Yes.
Q Do you know approximately how many credit cards were in these files?
A All -- just these two?
Q Yeah.
A I don't know, off the top of my head; hundreds.
Q Hundreds, approximately?
A Yes.
Q You mentioned you had found hacking tools on the HopOne server, also.
What type of tools did you find?
A Specifically, there were tools for scanning large sections of IP addresses. Found the -- some of the malware associated with kameo.
Q I'm showing you Exhibit 3.30; do you recognize that?
A Yes.
Q How do you recognize that?
A The first one is a screenshot of a batch file that I located on the system. And then the lower image is me actually executing that file on a government computer to show what it does.

MR. BARBOSA: Government offers Exhibit 3.30.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 3.30 was admitted)

BY MR. BARBOSA

Q Let's focus in on the top.

So where did this forensic artifact come from?

A So this was a batch file, or a small script, that could be run from this computer.

Q And what does this tell you, based on your training and experience? What would this script do?

A Okay. So if we kind of -- we'll have to just break it down. So the first part of it is the path to the actual executable file. So we see it's -- from the "C" drive. There's a folder called "RDP." Inside that folder is another folder called "work." And inside that folder is a program called "vnc.exe." I know vnc.exe, because I've used it.

And what it's saying -- the "-i" says, I want you to scan a range of IP addresses. And the first IP address in that range I want you to scan is 66.0.0.1. And I want you to scan from there all the way to 66.0.255.255. So that means that it would scan the 0.1, 0.2, all the way through 0.255, and then it would start with "1" and then through 255. So all total, that represents about 64,000 IP addresses that are going to be scanned.

The "-p" means that I want you to scan for a specific port. And in this case, it's Port 3389. And then the remainder of it has to do with how much -- how many threads or how much of the server load the user wants to contribute to this application. And they chose 400 threads, 400 at a time.

Q I'm going to bring up what was previously admitted as Exhibit 6.22, on the right-hand screen, this list of IPs.

How does that relate to what you see in Exhibit 3.30 from the HopOne server?

A So this is the abuse complaint that had come in. And so, basically, we see an abuse complaint for the behavior that would have occurred from running this batch file, just on a different set of IPs. But this would -- running this against this IP would have generated the exact same activity.

Q Was this abuse complaint for the same HopOne server you found the tool on?

A It was for a different server.

Q Did you examine that server, also?

A Yeah.

Q And did you find these tools?

A Yes.

Q Now, showing you what's been marked as Government's Exhibit 3.18, do you recognize this?

A Yes.

Q How do you recognize this?

A This is a remote desktop file that was pre-configured on one of the HopOne servers.

Q And was this -- is this in the same condition as when you found it on the HopOne server?

A Yes.

MR. BARBOSA: Government offers 3.18.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 3.18 was admitted)

BY MR. BARBOSA

Q Can you explain to the jurors what Exhibit 3.18 shows you, based on your training and experience?

A Can I explain how remote desktop works to explain this?

Q Well, let me ask you. Could you explain?

A So when you want to make a remote desktop connection, there's a couple ways to do it. If it's a new system that you haven't connected to before, you would launch the remote desktop program on your computer. And you would tell it, I want to connect to this IP, or this domain name, and I want to use this username and this password. And it would try to connect, if you were successful.

Now, if you're frequently connecting to the same remote system, like, it's your business's server, and you need to use it a lot, you can create a shortcut file that you can just double-click on, and it will automatically open up that remote

desktop connection. And typically, all you would then have to do is type in the password.

So what this is is -- so that would be represented with just, like, a computer icon on your desktop. So this is what the contents of that icon file are. And so it shows that if you had double-clicked on this default RDP icon, it would have connected to IP address 24.105.183.226. And it would have used the domain of "rentalplus" to do that.

Q Where was this shortcut located on the HopOne server?

A It was located in the "My Documents" folder for the shmak account.

Q And was that the same name as the user account that was logging in to the system?

A Yes.

Q Were you able to identify that IP address, 24.105.183.226?

A Yes.

Q Taking you back to Exhibit 6.12.

A It's Line 25.

Q What was that business?

A Finger Lakes Premiere Properties.

Q And Track 1 and Track 2, is that the type of data you found?

A Yes.

Q Where were they located?

A On the HopOne server.

Q Sorry. Where was the business?
A Rochester, New York.
Q As part of your examination of the HopOne server, were you able to figure out how these tools had been placed on the server?
A Some of them, yes.
Q How did you figure out how some of them had been placed on the server?
A Through the internet history.
Q What did that internet history show you?
A It showed that some of the tools had been downloaded from the FVDS server.
Q I'll ask you to get down from the stand again, let you stretch your legs a minute.

Could you demonstrate -- or explain for the jurors, using Exhibit 17.7, the path of these tools from the FVDS server to the HopOne server?
A Sure. So this was a tool staging server, so it had a lot of different malware and hacking-related tools that were on it. So they were downloaded from this server onto this server via a web browser.
Q I've brought up Exhibit 3.4. You can take your seat again. And tell me if you recognize that exhibit.
A Yes.
Q How do you recognize that?

A This is internet history from the HopOne server.
Q Does that fairly and accurately represent a portion of the internet history?
A Yes.
MR. BARBOSA: Government offers Exhibit 3.4.
MS. SCANLAN: May I inquire?
THE COURT: You may.

VOIR DIRE EXAMINATION

BY MS. SCANLAN
Q Detective Dunn, is this a portion of the internet history that you cut and pasted to make an exhibit, or did you create -- is this something you created, a list of entries?
A No. I cut and pasted this from the forensic tool. I didn't make this -- so I highlighted the ones that were applicable and made this exhibit.
Q So there's a whole bunch of internet history. I'm just trying to ascertain whether these were all together, as a piece of the forensic examination, that you put over, or whether you picked out pieces and put it over here.
Is this making sense, or no?
A It's not making sense, no.
Q Okay. So you have the whole internet history; right?
A Yes.
Q All this stuff?
A Yep.

Q Did you select these four and move them as a group, or are these pieces that you selected out of that longer internet history?

A Oh -- no. What I did was, with the forensic software, I can click on the entries that I want from the whole of the internet history, and then I can sort -- put them at the top and just export those four lines.

MS. SCANLAN: I have no further questions, and I have no objection.

THE COURT: Counsel, I don't have 3.4 in our materials.

Never mind, Counsel. It's admitted.

(Exhibit 3.4 was admitted)

MR. BARBOSA: Thank you, Your Honor.

DIRECT EXAMINATION

BY MR. BARBOSA

Q Detective Dunn, what is the internet history we're looking at here?

A So we're looking at the downloading of a number of files from shmak.fvds.ru to the HopOne server. Files specifically are pak4.exe, rdp.exe, and then server.rar.

Q Have you examined any of these files?

A Yes.

Q What did you find about them?

A Pak4 was a file that, if you executed it, would open up

additional malware. It was just a self-extracting executable. RDP is a remote desktop application. And then server.rar had the server files to set up the collection server.

Q What does the column "name" indicate here? What is this telling you?

A There are multiple sources for the internet history. And so that's just showing which piece of internet history that came from.

Q And the "last accessed," why did you include the last accessed on this particular exhibit?

A I don't remember.

Q Is that a date --

A It's a date that's associated with some of those files.

Q And these last accessed dates, you'd discussed these not being one that you use, typically.

Why is it used in internet history?

A The last accessed date, with internet history, can be a little bit difficult, because it can include the time that the actual overall internet history file was last accessed.

Q I see.

Moving to "internet artifact type," what does this column tell you?

A It tells me the type of artifact that it was. So the first one came from the registry, because it was a URL that was manually typed in.

Q The second one?
A Is its cached internet history, so it's saved in the index.dat file.
Q What is cached internet history?
A Your computer will save a certain amount of internet history as a record of your history.
Q And then downloads?
A That's from a different browser, Firefox, and it just shows that that was in the downloads history file.
Q And finally, "history"?
A It's the Firefox internet history.
Q So are these possibly two different browsers, types of browsers being used?
A Yes. And we can see that on the far column.
Q In addition to being used for collection of stolen credit cards, did you determine that the HopOne server had been using for other internet browsing besides this shmak.fvds.ru browsing?
A Yes.
Q How can you go about using a remote server to browse the internet?
A So you can connect to that remote server, and you're presented with a desktop that looks just like any other desktop, which includes an internet browser. And you can launch that internet browser and surf the web.

Q If you surf the web using a remote server, the internet site that you visit, what IP address will they see coming into their site?
A The IP address of the server that you're accessing.
Q What will that do in terms of their ability to determine where the original connection came from?
A It will prevent them from knowing.
Q Is there a term for that in your --
A It's called proxying.
Q What type of internet browsing history did you find on the computer?
A There was access to e-mail accounts. There was internet traffic related to travel, bookings of plane tickets.
Q Were any of those accesses to e-mail accounts of interest to your investigation?
A Yes.
Q What were they?
A There was a login to the e-mail account "boooks," which is B-O-O-O-K-S, "cafe@yahoo.com."
Q How much -- how often did you see that come up in the internet history?
A I just saw it maybe a handful of times.
Q Turning your attention back to Exhibit 17.7, did that -- that's the big board, if you could step down for a moment.
A Oh, sorry.

Q Did this booookscafe@yahoo.com come into your investigation later?
A Yes.
Q Can you explain how?
A Ultimately, we got a search warrant for the content of the booookscafe e-mail account, which showed that it was used to lease the shmak and smaus server. There was also a lot of other content in that mailbox.
Q So is that shown on the left-hand side there, connected to --
A Yeah. It's right here (indicating). The receipts for this server were in this mailbox.
Q You can go ahead and take your seat again.
And when you get there --
A And then this mailbox was accessed from this server (indicating).
Q Excellent. Thank you for pointing that out.
Do you have the binder with Exhibits 3.5 through 3.11 in front of you?
A Yes.
Q I'd like you to take a look at those. Let me know if you recognize them.
Are they additional internet history exhibits?
MS. SCANLAN: I'm sorry. Are we looking at 3.5 through 3.11?

MR. BARBOSA: Yes.

THE WITNESS: Yes.

BY MR. BARBOSA

Q Do you recognize all of those?

A Yes.

Q How do you recognize them?

A This is internet history that I extracted from the HopOne server.

MR. BARBOSA: The government offers Exhibits 3.5 through 3.11.

MS. SCANLAN: No objection.

THE COURT: They're all admitted.

(Exhibits 3.5 through 3.11 were admitted)

BY MR. BARBOSA

Q Let's start with Exhibit 3.5.

What did you find here?

A So this is internet history showing the computer accessing the site secure.bulba.cc, specifically viewing a ticket, like a help ticket.

Q Based on your training and experience, do you have an opinion on who would be able to view help tickets on that site?

A An administrator of the site.

Q What's an administrator?

A Somebody who's in charge, who's running it.

Q Moving to Exhibit 3.6, what do we have here?

A This is internet history related to the site track2.name. So we have access to secure.track2.name. We have an admin check extended logs visit, admin summary, profile login, and a ticket.

Q Again, based on your training and experience, what did this internet history tell you about the relationship between the user of the HopOne server and the track2.name site?

A That this user was an administrator on the server.

Q What about this exhibit told you that?

A The fact that they were accessing areas on track2.name that were not part of the user purchasing experience. These are admin functions.

Q Moving to Exhibit 3.7, what do we have here?

A Visits to track2vip.tv.

Q Was that one of the alternate domains that you pulled registration records for?

A Yes.

Q Moving to Exhibit 3.8, what do you have here?

A So these are web traffic to the site ozon.ru and orders for travel.

Q Do you know what the site ozon.ru is?

A Do I know the --

Q Do you know what ozon.ru is?

A It's a Russian travel site.

Q Why did you select internet history related to a Russian

travel site?
A Because a person booking travel would be very likely to put their real name and other travel documents.
Q Moving to Exhibit 3.9, what do we have here?
A This is somebody visiting the website fibotradepro.com, with a username of "smaus."
Q And why were you focused on that?
A Because that was a common username that I had seen throughout the case.
Q Were you looking on the HopOne server for evidence of other usernames or passwords?
A Yes.
Q I'm going to take you to Exhibit 3.10.
What do we have here?
A These are Bing searches for track2.tv and track2vip.tv.
Q Based on your training and experience, do you have an opinion as to why the user of the HopOne server would be searching for these sites, after having browsed to them?
A To see how well they were ranked on bing.com, like, where they show up in the search results.
Q What would the purpose of that be?
A The higher in the search results, the more likely somebody is to click on your site.
Q Finally, we have Exhibit 3.11 that was just admitted. This one is three pages long.

What is the internet history reflected in Exhibit 3.11 related to?
A The website carder.biz.
Q What was the website carder.biz?
A Carder.biz was another URL for the carder.su site. So it's a carding site.
Q And you're familiar with that site?
A Yes.
Q What was the content of the carder.su site?
A It's a credit card forum.
Q And what did this internet history relate to?
A A person searching on that site and viewing various pages, specifically a thread about bulba.
Q Were there threads about track2, also?
A Yes.
Q What does this tell you about what the user of the HopOne server was surfing to?
A That they were reading what was being said about track2 and bulba.
Q So while searching the HopOne servers, did you find any evidence related to who might be using these servers?
A Yes.
Q What type of evidence did you find related to the identity of who was using them?
A I found airplane travel records.

Q Showing you what's been marked as Exhibit 3.16.

THE COURT: Counsel, before you go there, let's let the jury stand and stretch.

Please be seated.

You may inquire.

BY MR. BARBOSA

Q Do you recognize Exhibits 3.16 and 3.16A, that are on the screen in front of you?

A Yes.

Q How do you recognize those?

A This is a cached internet page for travel records. There's the way I found it in Russian, and there's a translated copy.

Q Where did you find these?

A These were on the HopOne server.

MR. BARBOSA: Government offers Exhibits 3.16 and 3.16A.

MS. SCANLAN: No objection.

THE COURT: They're admitted.

(Exhibits 3.16 and 3.16A were admitted)

BY MR. BARBOSA

Q So I have Page 2 of each of these exhibits up for you. The translation is on the right.

What did you see in this?

A That they were an order for a plane ticket from Denpasar,

Indonesia, to Singapore, for two subjects, Roman Seleznev and Nina Udatova.

Q Did the record provide any other identifying information for Mr. Seleznev?

A Yes. It provided a date of birth and a passport number.

Q And have you seen Mr. Seleznev's Russian passport?

A Yes.

Q Does the passport information in that record, that you found on the HopOne server, does it match Mr. Seleznev's actual passport seized from him?

A Yes. Both the date of birth and the passport number match, as well as the expiration date.

Q How would -- based on your training and experience, how would a record like this end up on a HopOne server?

A Somebody would have logged into the HopOne server. Utilizing the web browser on the HopOne server, they would have traveled to -- or visited the Ozon travel website and booked this plane ticket.

Q So turning to Page 1 of this exhibit, what was the notation at the bottom of the first page of that Ozon record?

A "Welcome, Svetlana Selezneva."

Q Do you know who Svetlana Selezneva is?

A Yes.

Q Who is she?

A She was Roman's wife.

Q How do you know that?
A I've met her in person.
Q I'll show you a translation of Mr. Seleznev's internal passport.
Turning your attention to Page 5 -- 3, sorry -- is Ms. Seleznev listed in his internal Russian passport?
A Yes, she is.
Q How is she listed?
A "Registered dissolution of marriage with Selezneva Svetlana Alekseevna; 25th of July, 1986, her birthday. And the marriage was dissolved on November 7, 2012.
Q So turning back to Mr. Seleznev's international passport, did you find travel stamps in his passport that matched this reservation you found on the HopOne server?
A Yes.
Q Again, the name that was traveled in, in Exhibit 3.16A?
A Yes.
Q What was that?
A Roman Seleznev.
Q The date of birth?
A July 23, 1984.
Q And this passport number, was that the same as the one we're looking at on the left-hand side, 12.7A?
A Yes, that's correct.
Q Did the travel stamps in his passport match these dates

and arrival and departure airports that you see?
A Yes.
Q Did this passport number and date of birth, that we see in 3.16A, did this also show up in the Western Union records that you've seen earlier?
A Yes, it did.
Q Again, if you could step down and look at the chart here.
If you could explain for me where this phone number has shown up elsewhere in your investigation, using that chart.
A Sure. So the phone number itself showed up in the rubensamvelich e-mail account. The phone number showed up in the internet history on the HopOne server. The name and passport number were also on the HopOne server.
Q Okay. Is that all? You can go ahead and take your seat.
Did you find any other instances of the name "Roman Seleznev" on the HopOne server?
A Yes.
Q Showing you what's been marked as Government's Exhibit 3.15, do you recognize this?
A Yes.
Q How do you recognize this?
A It is a page from a website, ebaytoday.ru.
Q And where was this found on the HopOne server?
A In the internet history.
MR. BARBOSA: Government offers Exhibit 3.15.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 3.15 was admitted)

BY MR. BARBOSA

Q Where does Mr. Seleznev's name appear on this exhibit?

A Toward the top, in the middle, where it says "Seleznev, Roman."

Q Do you know what ebaytoday.ru is?

A What the site specifically is, no. It's related to eBay.

Q How would this type of internet artifact end up on a computer?

A Somebody would have logged into that site with the name of "Roman Seleznev."

Q From the server?

A From the server.

Q Why does this particular artifact not have all of the photographs in full rendition of the site?

A Because when I extracted it, my forensic tower was not online and couldn't grab those from the remote server.

Q And is that typical, how you practice your forensic examinations, you don't connect to the internet?

A That's correct.

Q So this is only data that was still remaining on the computer?

A Yes.

Q Did you find names other than "Roman Seleznev" or his wife's name, "Svetlana Seleznev," on the computer?
A Yes.
Q Do you recall what names those were?
A Yes.
Q Which -- what were some of the names that you found?
A Anton Gapanov, Alexander Khohlachev, Alex Smulskaya -- I can't remember his wife's name -- Eva Seleznev, Nina Udatova (phonetic), off the top of my head. There's more but --
Q Did you follow up on those names to determine if they might be the ones operating the HopOne server?
A Yes.
Q Did they cause you to change your focus of your investigation in any way?
A No.
Q Showing you what's been marked as Government's Exhibit 3.17, do you recognize that?
A Yes.
Q How do you recognize that?
A This is an Ozon travel record for Anton Gapanov.
Q Was that also found on the server?
A Yes.

MR. BARBOSA: Government offers Exhibit 3.17.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 3.17 was admitted)

BY MR. BARBOSA

Q Where did you find the name of "Anton Gapanov" in this record?

A Towards the bottom, on the left-hand side.

Q Now I'm going to show you Government's Exhibit 15.13.

MR. BARBOSA: The government will offer that exhibit under a 902 certification, Your Honor.

THE COURT: Any objection beyond those previously made, Counsel?

MS. SCANLAN: Is it more than one page?

MR. BARBOSA: It's five pages, yes.

MS. SCANLAN: I'm sorry, Your Honor. Let me pull --

THE COURT: That's all right.

MS. SCANLAN: Your Honor, the defense would suggest that there's a number of redactions that would be necessary for this exhibit to be submitted as substantive evidence.

THE COURT: All right. Counsel, why don't you conduct your examination without admission of the exhibit, and we'll address the redactions at the appropriate time.

BY MR. BARBOSA

Q Do you know who Anton Gapanov is?

A Yes.

Q Who is he?

A He is Roman Seleznev's friend and --

MS. SCANLAN: Objection to the basis of the information.

THE COURT: Counsel, I'm not sure about the entirety of your objection.

MS. SCANLAN: I'm sorry, Your Honor. The objection is the basis of this witness's information regarding who Anton Gapanov is in relation to Mr. Seleznev.

THE COURT: Members of the jury, why don't we just take an early lunch break. I'll take care of this, and I'll see you at 1:30.

(Jury exits the courtroom)

THE COURT: All right. Counsel, first let's hear your proposed redactions and let's hear the objection to the witness's testimony regarding identification or the relationship to this individual.

MS. SCANLAN: Your Honor, I understand the purpose of Exhibit 15.13 to be the -- identifying Anton Gapanov's name here, his visitation. The problem with this -- I don't have an authentication objection to this exhibit. The problem is the prejudicial nature of some of the information. So this indicates that Mr. Seleznev is at the Federal Bureau of Prisons, for instance. And then also all of the personal -- I'm not sure Mr. Calfo would appreciate his home address and his phone number being submitted to the jury, along with the

rest of these people who were visiting. So I do think that should be redacted. I would have assumed that that information would be taken out.

That's the objection to the exhibit. It's not the authentication of it. It's the information that's in it that's either sensitive or prejudicial.

THE COURT: Okay. Counsel for the defense -- one other question, Counsel, you're objecting to this witness's testimony about his familiarity or ability to identify the relationship between Mr. Seleznev and an individual in this document.

MS. SCANLAN: Correct.

THE COURT: And the nature of your objection?

MS. SCANLAN: I don't -- I don't think this witness has adequate personal information to say that Mr. Seleznev is friends with Mr. Gapanov.

THE COURT: Okay. Let me hear from the government. Thank you.

MR. BARBOSA: Your Honor, we don't have a problem with certain redactions. This is not Mr. Calfo's home address, but we're happy to redact some of that information.

In terms of the witness's knowledge, it is based on the exhibit. And this is a statement of the defendant. It's his contact list, and he has listed the relationship as friend. So I think -- I don't really need the detective to say this. But

assuming the record comes in, which I believe counsel has conceded it's authentic and it should come in, just with the redactions, I think that will satisfy everything.

THE COURT: Well, one, I don't think Mr. Calfo would object to free advertising. But setting that aside, I think it is appropriate for certain redactions to be undertaken. And I'm not going to get into nitpicking, but I do believe that the reference to the Federal Bureau of Prisons, that type of information, personal identifiers, should be deleted. And also, I don't know that it's relevant, that you need to put the relationship, because it gives the appearance that the defendant's had other attorneys connected with him. I don't know how relevant that is to the case.

MR. BARBOSA: Would you like me to just excise out attorneys from this list?

THE COURT: I think that's, at a minimum, Counsel, appropriate.

What other specific information do you need to have that establishes what you're trying to offer to the jury?

MR. BARBOSA: Mr. Gapanov's entire entry.

THE COURT: And that's on Page 1?

MR. BARBOSA: Yeah.

THE COURT: And just that page?

MR. BARBOSA: Yes. But also, we have another contact that we will discuss after the break, listed at the bottom of

Page 2, Alexander Khohlachev. And I think we can redact the remainder.

MR. BROWNE: Are you going to redact the "Federal Bureau of Prisons inmate" word, also?

MR. BARBOSA: Yeah. In fact, I think we can redact everything beyond Page 2. We can take Pages 3 through the end out.

THE COURT: And then on the first page, Counsel, you'll take the caption?

MR. BARBOSA: Yes.

THE COURT: And then also it says "inmate number."

MR. BARBOSA: Yes.

THE COURT: And it also says "inmate registration number."

MR. BARBOSA: I'll take that out too.

THE COURT: And "facility" and "institution."

MR. BARBOSA: Certainly. We will have those all redacted before the end of the break.

THE COURT: Counsel, I think that takes care of the bulk of your objection.

MS. SCANLAN: Yes, Your Honor. I would just ask that we can see the redacted exhibit prior -- before we start again, to save time.

THE COURT: Absolutely.

MS. SCANLAN: And beyond the fact that this says -- I

have two things. Beyond the fact that it says "friend," I don't think the detective can actually start testifying about the relationship between these two people based on what's in the record. He can say that's what's in the record, but not beyond that. He doesn't have information beyond that.

The other thing is that I would just inquire as to how the government -- what the government is going to say this is. So this is a list of what? In other words, so that they don't end up telling the jury that Mr. Seleznev is in custody.

THE COURT: What's the government plan on doing?

MR. BARBOSA: Well, we planned to use the exhibit. But we can -- the witness is here. I think we can just simply instruct the witness not to refer to it as an "inmate contact list," but as his "contact list."

THE COURT: And how will he establish that he has personal knowledge that he can connect Mr. Seleznev to this person?

MR. BARBOSA: He doesn't have to. The record speaks for itself. I only intended to ask -- I didn't intend to ask him that question until the exhibit was briefly excluded. So I only want him to point out that this person is listed by Mr. Seleznev in his contact list as a friend.

THE COURT: All right. Any objection to that, Counsel?

MS. SCANLAN: No.

THE COURT: That appears to resolve the problem. And the witness is specifically instructed not to make reference to the fact that Mr. Seleznev is or has been in custody.

THE WITNESS: Okay, Your Honor.

THE COURT: All right. Anything else to take up, by counsel for the government?

One other thing, Counsel, I'm still having trouble with 5.3 because the defense hasn't provided a brief or any case authority whatsoever on that, so I don't have the benefit of anything other than just an objection by the defense.

The case that the Court referred to, and the reason the Court's taken a pause, is, that dealt with circumstances where it was just a ledger that was identified. And that was permitted by the Court. The circumstances before the Court now, we have ledger plus, the "plus" being images or photographs. That's significantly different from the circumstances of the case that was presented to the Court for a separate independent identification; because that enhances the likelihood that this is truly being offered for the truth of the matter, as opposed to not.

MR. BARBOSA: Your Honor, the objection only applied to the written word. Counsel specifically indicated that the image -- they were not objecting to the images. And there are two different analyses. Photographs are not statements. They are unquestionably not hearsay. They just don't come under the

rule at all.

In terms of the commentary to it, again, this still comes under the circumstantial evidence of the connection to the account. And they're much less problematic than, for example, a drug ledger. A drug ledger, the statements in a drug ledger, are so much more assertive than the statements that we see in just the titles for these photographs.

THE COURT: So I'm clear, what the government intends on offering under 5.3 is the images and the account, not the content of the communication; is that correct?

MR. BARBOSA: We intend to offer the content of the communication, but not for its truth, but to prove that -- as circumstantial evidence of the defendant's connection to the account; because his wife's photographs are in the account.

THE COURT: Do you need anything -- let me pull 5.3 up again.

MR. BARBOSA: Your Honor, I believe it's analogous to a receipt found at a crime scene with a name that connects the defendant to the crime scene. Here, the name -- it's not even a name. It's just the word "daddy." And I think that's the primary objection. But if a receipt was found at a crime scene with the defendant's daughter's name, it would be admissible to prove the defendant's connection to that crime scene under the theory in the cases we've cited. It is circumstantial evidence of the defendant's connection to the crime scene, which is,

that is our theory of admission.

MS. SCANLAN: And I think if you -- in that case, if you had proved that that was that person's daughter in advance, and you could make that connection, then perhaps. But that is not what this is. So this language is offered for the truth of what it -- the connection that it's creating. I don't understand this new exception for things that are true but also happen to create a connection. That doesn't make it any less hearsay.

THE COURT: Counsel, the problem I have is that it's a double-edged sword, because you're offering it not for the truth, but then, in fact, you are offering it specifically to establish the direct relationship between the defendant and the individuals projected in the images.

Counsel, I'm giving the government the opportunity, if you want to redact the language that's reflected in 5.3, as an alternative, that will be a consideration by the Court. Because I agree with you that the images themselves aren't hearsay testimony. But I've got grave reservations otherwise, because I think we're starting to mix what is being offered for the truth, particularly when you have photographic images. And I don't have any case authority that goes as far as what the government's proposing to the Court.

MR. BARBOSA: And just to be certain I've been clear about this, we believe that is a carve-out for the hearsay;

that the circumstantial evidence of connection to the account allows this. But I understand the Court's ruling.

THE COURT: All right. Your record is made, but that's the Court's ruling.

Anything else to take up?

MR. BARBOSA: Well, let me -- I have this exhibit up now.

Specifically, what would the Court request we redact?

THE COURT: You can leave "Svetlana." You can leave "boookstorecafe" [sic]. But the content of everything from the attachments -- the attachments and beyond.

MR. BARBOSA: Okay.

THE COURT: I think that addresses the defense objection; is that correct, Counsel?

MS. SCANLAN: Yes, Your Honor.

THE COURT: All right. Then we'll be in recess.

Anything else to take up?

MS. SCANLAN: No.

MR. BARBOSA: No, Your Honor.

THE COURT: All right. We'll be in recess.

(Recess)

THE COURT: Good afternoon, Counsel.

MR. BARBOSA: Good afternoon, Your Honor.

THE COURT: You may continue your direct examination.

MR. BARBOSA: Thank you.

BY MR. BARBOSA

Q Detective Dunn, when we broke, you had just reviewed Exhibit 3.17A, and you indicated that you found the name "Anton Gapanov."

Exhibit 15.13, which was admitted shortly after the jury was excused, could you indicate whether you see the same name, "Anton Gapanov," in this -- in defendant's contact list here?

A Yes, I do.

Q What is the relationship defendant listed for Anton Gapanov?

A Friend.

Q And did the defendant list an address for Mr. Gapanov also?

A Yes.

Q Where is that?

A It's in Vladivostok, Russia.

Q Did you find any other instances on the HopOne server where the defendant's name appeared together with Mr. Gapanov?

A Yes, I did.

Q I'm going to show you Exhibit 3.24.

Do you recognize this?

A Yes.

Q I'll bring this on one screen.

How do you recognize this?

A This is data from the "page file" from that server. It

includes a number of different names, a little difficult to read.

Q Is that in the same format as you found it on the HopOne server?

A That's correct.

MR. BARBOSA: The government offers Exhibit 3.24.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: 3.24 is admitted.

(Exhibit 3.24 was admitted)

BY MR. BARBOSA

Q You said this was in the page file.

Is that indicated in the full path title up here?

A That's correct.

Q Can you explain to the jurors what "page file" is?

A Sure. So a computer has a number of different types of memory. There's the computer hard drive, which stores data. And then there's the computer RAM, which is the memory the computer is using when it's processing data. RAM is much smaller than the hard drive. And so when the system is running out of RAM, it will store that overload data temporarily in what's called the "page file.sys."

Q All right. The page file that you have here in Exhibit 3.24, based on your training and experience, what was this?

A This is on overflow internet history-related data.
Q And what type of internet history-related data was it, based on your review?
A It was related to flight itineraries.
Q And did it contain the names related to the flight itinerary?
A Yes.
Q Which names did you find?
A Roman Seleznev and Anton Gapanov.
Q Where is Mr. Gapanov's name, if you could direct me to that? Is this what I've highlighted down here?
A Yeah, there you go.
Q How does this type of data remain on the system?
A The page file.sys is not deleted when the system is powered off. The data will remain there until the system needs to use the page file again, at which point it will be overwritten. So it remained here, because the system didn't need to use that file again.
Q Did you find other information in the page file data?
A Yes.
Q Showing you what's been marked as Exhibit 3.19, do you recognize this exhibit?
A Yes.
Q What is this?
A This is additional travel-related records that were found

in the page file.

MR. BARBOSA: Government offers Exhibit 3.19.

THE COURT: Any objection?

MS. SCANLAN: Is it just the one page?

MR. BARBOSA: Two pages.

MS. SCANLAN: No objection.

THE COURT: All right. 3.19 is admitted.

(Exhibit 3.19 was admitted)

BY MR. BARBOSA

Q Drawing your attention to the first entry in Exhibit 3.19 from the page file, what do you have here?

A An e-mail address and a phone number.

Q What was the e-mail address that you found?

A Romariogro1@mail.ru.

Q And what was the phone number that you found?

A +74232550150.

Q Can you take a look at Exhibit 12.9, the paper documents that have already been admitted and were seized from the defendant at the time of his arrest?

A I don't have that in my binder.

Q It's -- this is a physical exhibit, bulky exhibit. Sorry.

THE CLERK: I'm sorry. Which exhibit, Counsel?

MR. BARBOSA: 12.9.

THE CLERK: Which exhibit is that?

MR. BARBOSA: That's the paper -- it's a stack of

papers and cards and documents.
BY MR. BARBOSA
Q Do those travel reservations that were on Mr. Seleznev's person contain the same e-mail address?
A Yes, they do.
Q I brought that up on the overhead, also, so you can highlight that for the jury.
What was that e-mail address again?
A Romariogro1@mail.ru.
Q Now I'm going to show you what's been marked as Exhibit 3.20; do you recognize this?
A Yes.
Q How do you recognize this?
A These are additional flight records from the page file.
MR. BARBOSA: Government offers Exhibit 3.20.
THE COURT: Any objection?
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 3.20 was admitted)
BY MR. BARBOSA
Q And what did you find in this page file data?
A This was travel records for Roman Seleznev on Transaero Airline, between Denpasar, Bali, Indonesia, and Moscow.
Q And where is Mr. Seleznev's name?
A It's the -- right there, the fifth line down.

Q And where did you find the travel -- the data regarding the travel?
A A little bit farther down. So the -- right there, Denpasar, Bali, on the 7th of July, to Moscow, DME.
Q Did you review defendant's passport to see if that travel was reflected in his passport stamps?
A Yes.
Q Turning your attention to Page 7 of his international passport, are those stamps reflected on Page 7?
A Yes.
Q Do they correspond with this reservation you found on the HopOne server?
A Yes.
Q Did you prepare a number of other exhibits with page file data that you retrieved from the HopOne servers?
A Yes.
Q Could you go through, in the binders in front of you, and tell me if you recognize Exhibits 3.21, .22, .23, .25, and .26? We've already admitted .24.
A Okay.
Q Do you recognize all of those?
A Yes.
Q Are they all additional page file data retrieved from the HopOne server?
A Yes.

MR. BARBOSA: Do you have objection?

The government offers 3.21, .22, .23, .25, and .26.

THE COURT: No objection, Counsel?

MS. SCANLAN: No objection.

THE COURT: They're all admitted.

(Exhibits 3.21, 3.22, 3.23, 3.25, and 3.26 were admitted)

BY MR. BARBOSA

Q If we could just go through these, I'd like you to direct me to highlight what information you found related to your investigation on each of these.

A The first one, the last name of "Seleznev," first name of "Roman," the birthday of July 23, 1984.

Q And did that match the passport that you've seen?

A Yes, it did.

Q Moving to Exhibit 3.22, what was the information that you had focused on in this?

A Last name of "Seleznev," first name "Roman"; date of birth, July 23, 1984; international passport. There's a second name in there, as well; last name, "Khohlachev," first name "Alexander"; birthday, April 6, 1985.

Q Did you see that name in defendant's contact list?

A Yes, I did.

Q Was that found on Page 2 of the contact list?

A That's correct.

Q And what was the relationship the defendant listed for

Alexander Khohlachev?
A Friend.
Q And what's his address?
A In Vladivostok, Russia.
Q Turning to 3.23, what were the names you found in here?
A There was -- there were a couple other names on the previous one, as well. I don't know if you wanted to --
Q Oh, 3.22?
A Yeah.
Q What other names did you find?
A "Smulskiy, Alexey."
Q Do you know who Smulskiy, Alexey is?
A That's Mr. Seleznev's --
MS. SCANLAN: Objection.
BY MR. BARBOSA
Q How do you know that?
A I've interviewed his daughter.
MR. BARBOSA: Withdrawn.
BY MR. BARBOSA
Q What other information did you focus on in Exhibit 3.23?
A The sixth line down, towards the far right, "Svetlana Selezneva."
Q Do you know who that is?
A Yes.
Q How do you know who that is?

A I've interviewed her.
Q Who is she?
A Roman Seleznev's ex-wife.
Q And is there another name down here?
A Yes.
Q What's the name that you find there?
A Eva Selezneva.
Q And I'll bring up Exhibit -- drawing your attention to 12.6B, a translation of Mr. Seleznev's internal Russian passport.

First, I'll draw your attention to Page 3, do you find the name "Alekseyevna Smulskaya" in there?
A Yes.
Q Is that the name you'd seen in 3.22?
A Yes.
Q And down to the bottom of this page, do you find any children listed for Mr. Seleznev?
A Yes.
Q Who do you have listed there?
A Eva Romanovna Selezneva.
Q Does that match the page file data that you found with Svetlana Seleznev's name in 3.23?
A Yes.
Q Is there a date of birth listed for Eva Selezneva?
A If you can make it bigger. Or -- I'm sorry. Which -- are

we in 3.23?
Q Yeah. A 2009 date?
A Yeah. There's 2009.
Q And does 2009 match up with the date of birth listed in the passport?
A Yes.
Q Moving on to 3.25, what was the information you found here?
A Very first line, last name "Seleznev," first name, "Roman"; birthday, July 23, 1984; last name "Khohlachev," first name "Alexander."
Q Additional name here?
A Sergei Nikulnikov.
Q And?
A Svetlana Selezneva.
Q Finally, 3.26?
A Svetlana Smulskaya, Alexey Smulskiy, Natalia Stepnova, Eva Selezneva. That's it.
Q Is there an "Eva" in there, or just the "Selezneva"?
A No, it's "Eva." The "7C" is part of the coding. It starts with the E-V-A. And there is her birthday, as well, 2009-4-19.
Q Does that match up entirely with the passport?
A Yes.
Q All right. Some pretty dense information there.

Let's move on to, in your investigation -- actually, not moving on, I think moving back a little bit -- I'd like to draw your attention to late October of 2010.

Were you notified of a possible breach at Broadway Grill in Seattle?

A Yes.

Q How had Broadway Grill been identified as a possible victim of a breach?

A A bank investigator had contacted me and advised that it appeared to be a common point of purchase for cards that were being used for fraud.

Q What did you do when you received that information?

A I responded to the Broadway Grill, and contacted the owners.

Q Who did you contact at Broadway Grill?

A Primarily, I spoke with CJ Saretto.

Q Were they aware of any problems?

A They had heard from a number of --

MS. SCANLAN: Objection. Hearsay.

THE COURT: Sustained.

MR. BARBOSA: It's not offered for the truth of the matter asserted, just to explain the investigation. That witness will also be testifying.

THE COURT: All right. The objection is overruled. You may answer the question.

THE WITNESS: They had heard from a number of customers, received complaints of fraud subsequent to being there.

BY MR. BARBOSA

Q What did you do when you went to the Broadway Grill?

A I received consent to create forensic images of a number of the point-of-sale systems, as well as the back-of-house server. I also captured the RAM memory from the system.

Q So what kind of exam was this? What type of forensic imaging did you do?

A I did live imaging. They were open for business at the time.

Q Did you leave their systems intact?

A Yes.

Q All right. Did you review the RAM while you were there, or did you take it back to your office?

A I took it back to my office.

Q Were you able to -- did you use all the same methods of conducting a forensic image, or creating a forensic image, as you described earlier?

A Yes.

Q And were you able to verify the integrity of the forensic images that you captured?

A Yes, I was.

Q When you returned to your office and conducted your

forensic examination, what did you find on the Broadway Grill's forensic image?

A I found the malware associated with this case was actively running on the system. I also found a file containing approximately 32,000 credit card numbers that had been exfiltrated from the server.

Q Did you review the RAM, as you had at Schlotzky's Deli, to determine if it was connected to any IP addresses?

A Yes.

Q What did you find in your review of the RAM?

A I found that the memory RAM from that server was connecting out.

Q Do you know where it was connecting out to?

A It would have been connecting to the FVDS server, I believe.

Q Let me bring up an exhibit to help refresh your recollection.

Can you take a look at Exhibit 1.2?

A I'm sorry. It was connecting to the server in the Ukraine.

Q Before we go into that exhibit, you said you found a file with credit cards in it.

How many credit cards were in there?

A Approximately 32,000.

Q Was that typical for a business computer system to have a

file with the credit cards in it?
A No.
Q Based on your training and experience, why would there be 32,000 credit cards sitting in a file on a system like that?
A That system was not configured correctly, and it was logging every card that had been scanned there. It was in what's called "full auditing mode."
Q How long had it been logging those credit card numbers?
A Years.
Q What did you find in terms of whether those had been compromised?
A I found that they had been compromised.
Q Can you explain how?
A They had been zipped up into a compressed format and exfiltrated out of the system, via the internet.
Q Did you find any -- you said you found malware on the system.
What was the nature of the malware you found?
A I found a version of the kameo family of malware.
Q So now let's turn to Exhibit 1.2.
What is Exhibit 1.2?
A This is forensic extracts from what I found on the Broadway Grill system.
Q And do these all accurately represent the forensic artifacts and extracts that you pulled from the Broadway Grill

system?
A Yes.
MR. BARBOSA: Government offers Exhibit 1.2.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 1.2 was admitted)
BY MR. BARBOSA
Q So starting with Page 1, in the top of Exhibit 1.2, can you explain to the jurors what we are looking at here?
A So this is records showing the downloading of the dtc2.exe malware onto the system, as well as accessing sendspace.com.
Q Based on your training and experience, what did this internet history tell you?
A That the malware had been downloaded from shmak.fvds.ru, and that the subject had also accessed sendspace.com.
Q What was the significance of the typed URL artifact type?
A It's the type of internet history that this was, meaning that somebody had actually typed in these web addresses into the web address bar, as opposed to clicking on a link.
Q So would somebody accessing these -- how would they know the address for this website?
A You would have to know the address off the top of your head, or had it written down.
Q If you could step down from the stand again to Exhibit 17.7, and explain how this relates to the diagram that

we've been using as our infrastructure diagram.
A So if this is the Broadway Grill, then we have somebody who's actively on this machine, so remotely accessed it. And they're typing in the address for this server to download the malware to this machine.
Q And then what does the sendspace internet history tell you?
A That they -- the stolen credit card numbers, that 32,000 cards that were on there, were uploaded to a sendspace.
Q What's the basis of that opinion?
A Based on the sendspace traffic that was there, as well -- and the timing of the sendspace, as well as the location of the -- or the discovery of the zipped files.
Q And what was the timing of this navigation to the shmak site and the sendspace site?
A They were within minutes of each other.
Q Was that both on October 22, 2010?
A Yes.
Q Turning to the second half of the page, 1 of 1.2, what is this file list we have here, on the second half of Page 1 of 1.2?
A These are the files of note that I found on the Broadway Grill server that were applicable to the events surrounding the hack.
Q What did you learn about these files?

A So do you want me to go in order of them?
Q Yes, please.
A Okay. So "sc.exe," with all the numbers, ".pf," that's a prefetch file. And it's called up at the same time that the sc.exe application is pulled up. If you recall from what I said earlier, "sc" is used to create the persistence mechanism, so that if the computer is shut down, when it's fired back up, that the malware will continue to run; as opposed to if it hadn't been created as a service, if the computer was turned off, when it came back on, the malware wouldn't run anymore.

The "RMCCAUDT.zip.lnk," that's a link file to the zip file that contained those 32,000 credit card numbers. So the file was zipped up to make it smaller and easier to exfiltrate.

Q Let me stop you for a minute.

So that zip file, had that been created by the Broadway Grill?

A No.
Q No? How had that been created?
A That had been created by the hacker.
Q So what was your opinion as to -- based on your training and experience and your exam, as to how the hacker had used this zip file?
A So the -- one of the reasons for using a zip file is because it compresses the data and makes the file smaller. So if you're trying to upload a file from that server somewhere

else, the smaller the file is, the faster you can upload it.
Q So moving on to "notepad.exe."
A Notepad.exe, that's again a prefetch for the notepad.exe. And it's my opinion that notepad was used to view the contents of the RMCC audit file.
Q Next?
A "Net1.exe" is a tool to view network connections on a computer.
Q And the highlighted Line 5?
A So this is dtc2.exe. Again, this is a prefetch file just showing that dtc2 had been run.
Q What was "dtc2"?
A That's the newer version of the kameo malware that was designed to upload stolen card numbers to the Ukranian server.
Q Why did you believe this was just a newer version of the same software?
A Because it was very similar in size, and the actual coding at the end only changed the dump server and actually made reference to kameo within the coding.
Q The naming convention "dtc" or "dtc2," did that have any significance?
A So there is a process within the Windows operating system called "distributed transaction client." So one thing that malware authors will do is to name their malware something that looks like a legitimate process. That way, if somebody, a

system administrator or something else, is looking at -- for a suspicious process running on the computer, it will look like it's supposed to be there.

Q What are the remaining pieces of malware that you found here?

A "Net.exe" and "cmd.exe" are both Windows applications. Net is -- has to do with networking, and cmd.exe opens up a command prompt. Dtca.exe, once you install dtc2.exe, it would rename itself to dtca and place itself in a particular directory for persistence. And then finally, there's the prefetch file, dtca.exe.

Q Were you able to review the actual code of dtca, like you had done at Schlotzky's on kameo?

A Yes.

Q What did you find in terms of similarities with the code you had seen at Schlotzky's Deli?

A That it was very similar. That the exfiltration server was coded the same. The only change was the IP address, but it was still sending data to the ftm.php script on the receiving server, and that it specifically mentioned kameo in the coding.

Q And what was kameo?

A Kameo was the version of malware that we'd found -- that I had found at Schlotzky's Deli.

Q The server we have with the IP address 188.95.159.20, could you explain, using the big board, where that would fit in

the diagram?
A Sure. So it's not on the diagram. It would have just been another server similar to the HopOne that would have received stolen credit card numbers.
Q And where was that geographically located?
A In the Ukraine.
Q So how many total collection servers had you identified at that point?
A Thirty-one in Russia, one in the Ukraine, and then one at the HopOne data center in McLean, Virginia.
Q You can go ahead and take the witness stand again.
Going back to the shmak.fvds.ru server that you had identified as having been the source of the malware, were you able to determine the IP address that's listed on Exhibit 17.7 as a demonstrative?
A Yes.
Q How did you go about figuring out what the IP address was?
A I ran a command on my work computer to trace the route of internet traffic from my computer to the shmak computer.
Q Showing you what's been marked as Government's Exhibit 4.13, do you recognize that?
A Yes.
Q How do you recognize that?
A It's a screenshot of the trace route that I ran to the shmak.fvds.ru server.

Q Does that accurately show the results of the trace route?
A Yes.
MR. BARBOSA: Government offers Exhibit 4.13.
MS. SCANLAN: May I inquire?
THE COURT: You may.
VOIR DIRE EXAMINATION
BY MS. SCANLAN
Q So Detective Dunn, what -- you ran a "traceroute" that created this.
Can you explain that?
A Sure. So you can -- one of the things you can do is, you can trace the route that your computer connection is going to take between where you are and where the final destination is, and it will show you all of the hops in between. So this is just showing me that I ran a traceroute to shmak, and that the final destination was 188.120.225.66.
Q And is this -- did you type this out, or is this --
A So my command would have been -- I would have typed out "traceroute," space, "shmak.fvds.ru." And then everything else -- basically the bottom line, where it says "traceroute to shmak.fvds.ru (188.120.225.66), 64 hops max, 52 byte packets," that's generated by the computer operating system.
Q Without reading the first two lines, are those computer generated, or what is that?
A Without reading --

Q There's four lines total; right?
A Yep. So the first line is me running the date command so that everybody would know what day I did this.
Q Okay.
A And then it prints the date out on Line 2. And then Line 3 is me running the trace route. And Line 4 is the -- showing me where the trace route is going to go.
MS. SCANLAN: No objection.
THE COURT: 4.13 is admitted.
(Exhibit 4.13 was admitted)
DIRECT EXAMINATION
BY MR. BARBOSA
Q So what did this tell you?
A It told me that shmak.fvds.ru was located at IP address 188.120.225.66.
Q Was that the same address you had seen in the Schlotzky's Deli malware?
A Yes.
THE COURT: Let's let the jury have a stretch break, Counsel.
Please be seated.
Please continue, Counsel.
MR. BARBOSA: Thank you, Your Honor.
BY MR. BARBOSA
Q At some point in your investigation, did you navigate to

the shmak.fvds.ru website?
A Yes.
Q Why did you do that?
A To see if there was additional malware there.
Q What did you find?
A That there was additional malware there.
Q What did you do?
A I downloaded that malware.
Q Why did you download that malware?
A So that we could determine if there were other or newer versions that we needed to look for, other dump servers, potentially.
Q How did you go about downloading the malware?
A The malware author used a common naming convention. And so between the names that we saw coded in the malware, as well as the fact that we were progressing from "dct2" to "dct4," I tried what would be common combinations.
Q And how much malware did you download?
A I downloaded a couple other samples.
Q And what did you do with those samples that you downloaded?
A I sent them to the United States CERT.
Q What is "United States CERT"?
A It's the U.S. Computer Emergency Response Team, based out of Pittsburgh, Pennsylvania.

Q And what was the purpose of sending them to CERT?
A To get a full reverse engineering report on the malware.
Q And do you know who worked on that at CERT?
A Matthew Geiger.
Q What did you do with the list of 32,000 card numbers that you believed had been stolen?
A I provided those to the card brands.
Q And did you provide -- did you receive records back from the card brands?
A Yes.
Q Did you pass those records from the card brands on to Ms. Wood?
A Yes.
Q Did you learn about other victim businesses during the course of your investigation?
A Yes.
Q Could you go over the various ways you learned or -- learned about victims, or identified victims in this case?
A So in addition to identifying victims through the servers that we were able to monitor and gain access to, we also worked with groups called "private forensic investigators." So as part of the PCI, or the payment card industry standards, there are private forensic companies that will respond to payment system breaches and conduct investigations. There are only about 14 of them in the U.S. that conduct these investigations.

And so I know folks that work there, and I spoke with them and asked them to provide me with any information on cases that were related to this family of malware.

Q And did you follow up on some of those?

A Yes.

Q A little bit more about private forensic investigations, why would a business have to have a private forensic investigation done?

A So when a business is -- becomes a victim of a point-of-sale intrusion, they are oftentimes required, by either their merchant acquiring bank or the card brands, to obtain a private forensic investigation to determine what happened and how it happened and, most importantly, the window for which card numbers were exposed, so that they can limit the losses on those cards. So they have to get that report done and then provide it to their merchant acquiring bank. And those are also provided to the card brands.

Q How much do those private forensic investigations cost?

A The cheapest I've ever seen one is for $6,000. And they can run, depending on the size of the merchant, upwards of $100,000. They average around $25,000.

Q Approximately how many victim systems did you examine personally?

A Approximately 20.

Q Did that include victims in the Western District of

Washington?

A Yes.

Q Do you recall which victims those were?

A I examined Village Pizza. I examined MAD Pizza on Thomas Street, MAD Pizza on First Hill, MAD Pizza in Madison Park, MAD Pizza in Tukwila, Casa Mia Italian Restaurant, the Broadway Grill, and the Grand Central Baking Company.

Q Can you tell the jurors generally what you found on the victim systems you personally examined?

A That the victim systems had been compromised via a remote desktop; that upon gaining access to the victim systems, that the hacker would then download the malware tool kit from shmak.fvds.ru; that the malware would then be installed on those systems. In some cases, after a month or two, the attacker would come back into the system and install an updated version of the malware to point the stolen card numbers at a new server.

Q Okay. And so what were the servers you identified? And it may help, if you need to, to get back down and use the diagram. What were the servers that the malware was pointing the stolen numbers to?

A So there is only one listed here, and that is the -- there's two listed here, actually. So the malware pointed stolen card numbers at the shmak/smaus.fvds server. They pointed card numbers at HopOne. And they also pointed card

numbers to a Ukranian address that started with 188.95.

Q Have you also reviewed an exhibit that diagrams out the victims you examined, or several of the victims you examined, with arrows pointing to where the malware was directing cards and where the malware was coming from?

A Yes.

MR. BARBOSA: May I approach, Your Honor?

THE COURT: You may.

MR. BARBOSA: Any objection to using this exhibit?

MS. SCANLAN: No.

THE COURT: What's the number, Counsel?

MR. BARBOSA: I've shown this to counsel at the break, and they've indicated they have no objection.

MR. BROWNE: We approve of it, Your Honor. I just wonder whether there's a number on it.

THE COURT: That's what I'm asking.

MR. BARBOSA: Oh, sorry. Exhibit 17.9.

MR. BROWNE: Okay. Thank you.

MR. BARBOSA: The government offers that as a demonstrative only.

THE COURT: And there's no objection, so it's admitted.

BY MR. BARBOSA

Q The computer icons down at the bottom, what do these represent?

A Each one of these is a different victim that was hacked into.
Q And what do the boxes at the top represent?
A The boxes at the top indicate the server from where the malware was downloaded, as well as the three servers for where the stolen card numbers were subsequently uploaded.
Q So was one of those servers serving both roles?
A Yes.
Q Which one was that?
A The shmak.fvds.ru server.
Q The arrows on this chart, what do they indicate?
A The arrows indicate the direction of flow of data. So the blue arrows show the downloading or uploading to the shmak, green for the Ukranian server, and red for the HopOne server.
Q And these flows of data, as you describe them, are they transmitted over the wires, over the internet?
A Yes.
Q So going from left to right, can you explain what you found, based on your forensic examinations, as to how the data was moving around?
A Sure. So for the Broadway Grill intrusion, the malware was downloaded from the shmak.fvds server, and the stolen card numbers were uploaded to the Ukranian server. For the Schlotzky's Deli, the malware was downloaded from the shmak.fvds server, and the stolen card numbers were uploaded

back to that same server. For the Grand Central Baking Company, the malware was downloaded from the shmak.fvds server, and the stolen card numbers were uploaded to that same server. For the MAD Pizza in Madison Park, the malware was downloaded from the shmak server and also uploaded. From the MAD Pizza on First Hill, the stolen card numbers were uploaded to the shmak.fvds server. Wasn't able to determine -- or confirm that the malware was downloaded from there. We just know that it was uploaded to -- the stolen card numbers were uploaded to there.

For the MAD Pizza in South Lake Union, the malware was downloaded from the shmak.fvds server, and the first version of the malware that was installed sent the stolen card numbers to the server in the Ukraine, and then another version of the malware was later installed, which sent the stolen card numbers to the HopOne server. The MAD Pizza in -- which we refer to as MAD Pizza Starfire, which was on Starfire Road, in Tukwila, downloaded the malware from the shmak server and initially uploaded to the Ukraine server and then later uploaded to the HopOne server. Casa Mia Italian Restaurant in Yelm, both downloaded -- downloaded malware and uploaded stolen card numbers to the Ukranian server. And then finally, Village Pizza uploaded to the Ukraine server and uploaded to the HopOne server, although we didn't have -- I wasn't able to find forensic artifacts indicating where the malware had been

downloaded from.

Q There's a lot of transmissions there. I think you may have made an error on Casa Mia.

Was that going to the Russia server or the Ukraine server?

A It went to the Russia server.

Q If you could take the witness stand again.

Did you prepare exhibits with forensic artifacts for each of the victim point-of-sale systems you examined for trial?

A Yes.

Q In general, what did you include in each of those exhibits?

A I included data related to the malware, data related to the passwords that were on there, data -- internet history for when the malware was downloaded from the system.

Q Okay. I'm going to ask you to take a look at Exhibits 1.3 through 1.9, in the binders in front of you, and let me know if you recognize those.

A Yes, I recognize these.

Q Do these all accurately reflect the forensic artifacts you found on the systems you examined?

A Yes.

Q Or on the select -- this is not every single system you examined; is it?

A No.

MR. BARBOSA: The government offers Exhibits 1.3

through 1.9.

THE COURT: Any objection?

MS. SCANLAN: I'm sorry, Your Honor. May I have one moment?

THE COURT: You may.

MS. SCANLAN: Your Honor, the defense would object that these are essentially just the written formulation of what the witness is saying. So he's going to say it, and then we have the written record of him saying it that becomes an exhibit; that that's improper by highlighting the testimony. It's just a written record of what he's saying.

THE COURT: The objection is overruled on those grounds. Exhibits 1.3 to 1.9 are admitted.

(Exhibits 1.3 through 1.9 were admitted)

BY MR. BARBOSA

Q I'd like to turn your attention to -- let's start with Exhibit 1.5. I don't know if we need to go over every one of these, but let's use this as an example.

Can you explain what you found in your examination of the systems from MAD Pizza Starfire?

A So the first -- the top half of this shows the internet history from this system. So it shows that on November 2, 2011, Internet Explorer was used to download dtc2.exe, which was the malware that uploaded to the Ukrainian server. And then 11/29, shmak.fvds.ru was visited to download the dtc4.exe

malware, which uploads to the HopOne server. And then the lower section shows the presence of those actual files on the -- on the hard drive.

Q Turning to Page 2 of this exhibit, what are the excerpts of code you included here?

A So this shows -- the very first one shows the dtc2 executable, and with the highlight for the server that would receive the stolen information, the Ukraine server, 188.95.159.20.

Q Is that the server in the center of the top on Exhibit 17.9, then?

A That's correct.

Q And then down lower?

A The second one shows the next version of the malware, dtc4.exe, which would upload the stolen card numbers to IP 66.36.240.69, otherwise known as the HopOne server.

Q The server on the right of Exhibit 17.9?

A Yes.

Q Okay. Moving to the bottom of this page, what do you have here?

A So I cracked the passwords for the user accounts on that system to confirm that they were the same as other Firefly systems that I had seen. And I -- this is just showing that the Firefly support user account had a password of "911fire." And the administrator password was "4Phoenix."

Q Why did this get your attention? Why were you focused on this password?
A Because the password was the same across all of the Firefly devices that I had examined, and the Firefly support account is the one that would have been used to access these devices remotely, via Port 3389, to administer them.
Q Did this cause you any concerns?
A Yes.
Q Why?
A Because if you don't have unique passwords on multiple different servers, if the hacker knows the password to one system, he knows the password to all of the systems.
Q Based on this finding, as you saw across different systems, did you form an opinion as to how the hacker was accessing all of these different restaurants and victims?
A Yes.
Q What was that opinion?
A That the hacker had the username "Firefly Support" and the password "911fire" in their dictionary.
Q Does each of these exhibits, 1.3 through 1.9, contain the exact same forensic artifacts?
A They're not exactly the same, but they're all very similar.
Q What are some of the key differences?
A Some may have a different version of the malware for -- I

don't know if we have Schlotzky's in here. Okay. So Schlotzky's has a different version of the malware, an earlier version. Some of the systems don't have dtc4 on them.

Q Looking at 1.6, MAD Pizza Starfire, which malware was used there?

A It just -- it had dtc2 and dtc4. It also had Telnet, which is another tool to remotely connect to a system.

Q Were there differences in the collection servers, also?

A There were only three collection servers.

Q Only three. Okay.

Were there occasional differences in the internet history?

A Yes.

Q Can you explain -- we're looking at Exhibit 1.8. Can you explain what you found here at Grand Central Baking Company?

A So in this case, instead of typing in shmak.fvds.ru, slash, the name of the malware, they just typed in the IP address for the server.

Q Is that a normal way to navigate to a website?

A No.

Q How would one -- what level of knowledge would one have to have in order to navigate directly with an IP address?

A You'd have to have a significant knowledge about that server.

Q And is this also a typed URL?

A Yes.

Q What does that tell you?
A That the user actually typed in that IP address.
Q The forensic artifact from Grand Central Baking, the location of where you found that, where was that?
A It was in unallocated clusters.
Q What did this tell you?
A It had been deleted.
Q And when do you believe it had been installed on their system?
A On October 22, 2009.
Q Did you also have internet history related to October 4, 2010, on the Grand Central Baking system?
A Yes.
Q Did you prepare -- instead of going through every one of these, did you prepare a summary of the malware installation and the mitigation dates?
A Yes.
Q Would it be easier to go over this with the summary?
A Yes.
Q I'm going to show you what's been marked as Exhibit 1.15.
Do you recognize that?
A Yes.
Q How do you recognize it?
A This is a summary exhibit that I created showing the installation and update -- malware update dates, if applicable,

as well as the collection server IP addresses and the mitigation dates.

MR. BARBOSA: The government offers Exhibit 1.15.

THE COURT: Substantive or demonstrative?

MR. BARBOSA: Substantive.

THE COURT: Counsel, any objection?

MS. SCANLAN: Yes, Your Honor. The defense renews our objection that this is not a proper summary exhibit.

THE COURT: The Court's previously ruled. Objection is overruled on those grounds. 1.15 is admitted.

(Exhibit 1.15 was admitted)

BY MR. BARBOSA

Q Can you go over the categories that you've included in this summary exhibit?

A Yes. So there's the victim, which is the victim business that was impacted; the malware installed date, so that's the date that the malware was installed on the system. There's the malware updated, so that is -- in three cases, the malware was updated to another version, and so that date is listed. The collection server IP address and location, so that's the IP address for where the card numbers were being sent. The mitigation date was the date that law enforcement contacted that business and told them that they had been hacked. And then the exhibit is the exhibit number.

Q So mitigation date, is that when the hack came to an end?

A Yes.
Q So based on all of your examinations, do you have an opinion on where the malware transmissions originated for each of the victims, including the one where you do not -- you do not have a direct piece of evidence in terms of internet history?
A Yes.
Q What is that opinion?
A That they came from the shmak.fvds.ru server.
Q And where was that located?
A In Russia.
Q And based on your examination of all these systems, were they transmitting the stolen credit card numbers to a location still within the Western District of Washington?
A No. They didn't transmit within the Western District. The transmission initiated here.
Q And where did they all end up in?
A Either in Russia, the Ukraine, or in Virginia.
Q Okay. During the time that the hacker has his malware operating on these systems, what level of control did that malware provide to the malware author or operator of the credit card numbers transiting that system?
A Can you ask that question again?
Q That was a terrible question. I apologize.
What authority did the malware give the hacker over the

victim computers?
A The ability to steal every credit card number that transited those systems.
Q So did the malware operator have the ability to control all of the numbers that were transiting the system?
A Yes.
Q Throughout the time period that it was operating?
A Yes.
Q How often did the malware transmit the stolen credit cards to the collection servers? Were you able to determine that?
A I was told by --
MS. SCANLAN: Objection.
MR. BARBOSA: Withdrawn.
BY MR. BARBOSA
Q You didn't do that analysis yourself?
A No.
Q Okay. I'm going to move on to a new topic.
At some point in your investigation, did you become aware of another online nic that you believed was related to Mr. Seleznev?
A Yes.
Q What was that other nic?
A Do you want me to spell it or --
Q Why don't you spell it first, and I'll ask you a follow-up question.

A "N-C-U-X."
Q And how is that pronounced?
A "Seek."
Q How did you come across the nic "nCuX," or "seek"?
A Through the search of an e-mail account.
Q And what e-mail account was that?
A The boookscafe@yahoo.com e-mail account.
Q Did you come across that nic in any chats that you reviewed -- chat logs that you reviewed on suspect computers in your case?
A Yes.
Q When was that?
A I reviewed those chat logs within the last month.
Q Did you -- had you seen copies of those chat logs before?
A Yes.
Q So was that part of your original investigation?
A Yes, absolutely.
Q Okay. Where did these chat logs come from?
A They were from a computer hard drive belonging to a credit card suspect in another case.
Q And who had possession of that computer hard drive? How did they come into law enforcement's custody?
A The Secret Service had the actual computer tower.
Q And were you able to review that actual computer tower?
A Yes.

Q And what did you look for?
A I looked for the Skype chat logs.
Q Did you find them?
A Yes.
Q Were you able to use the same tools and forensic analysis that you've discussed before?
A Yes.
Q So I'd like to show you Exhibit 16.2.
Do you recognize that?
A Yes.
Q How do you recognize that?
A This is the chat log that I extracted from that computer hard drive.
Q And does that fairly and accurately show the chat log as it existed on the hard drive?
A Yes.

MR. BARBOSA: Government offers Exhibit 16.2, which is three pages long.

MS. SCANLAN: Your Honor, the defense would object that the government has not established a sufficient foundation for this to be, I'm assuming, statements of a co-conspirator.

THE COURT: Counsel?

MR. BARBOSA: We're admitting this as a statement of a party opponent and statements of co-conspirators. The opposite side of the conversation is the statement of the

co-conspirator.

THE COURT: The objection is overruled on those grounds. 16.2 is admitted.

(Exhibit 16.2 was admitted)

BY MR. BARBOSA

Q This chat is three pages long. Can you explain what the subject of this chat was?

A It was in relation to the purchase of an MSR206.

Q Who were the parties to the chat?

A The parties were the nic, "uBuyWeRush," and the nic "nCuX111."

Q And MSR206, is that the same device you have there as the demonstrative on the stand with you?

A Yes.

Q Can you explain, again, what are those used for?

A For reading and encoding magnetic stripes on cards.

Q In this chat conversation, who is selling the MSR206?

A UBuyWeRush.

Q And who is buying it?

A NCuX111.

Q Did nCuX111 provide an address to deliver the device?

A Yes.

Q Where is that? Is that on Line 61?

A Beginning on Line 59, continuing through Line 61.

Q Can you read that into the record?

A "I need the" -- this is -- uBuyWeRush states, "I need the following: Complete shipping details." NCuX responds, "Okay," and then responds, "Name, Roman Seleznev; address, Ostryakova 26, Apartment 113, Vladivostok, Russia."

Q Did nCuX111 provide e-mail addresses, also?

A Yes, Line 65.

Q What were the two e-mail addresses provided?

A Regmails22@mail.ru and boooks -- B-O-O-O-K-S -- cafe@yahoo.com.

Q And where did that boookscafe account fit in on the diagram that you had gone over earlier, the track2 infrastructure?

A The boookscafe e-mail address had been found on the HopOne server.

Q The physical address that nCuX provided, the Ostryakova address, did you see that in defendant's internal passport?

A Yes, I did.

Q I'll bring that up so I can show it.

Was that the address that the defendant listed as his place of residence?

A Yes. "Has been registered at Ostryakova Street, Building Number 26, Apartment 113."

Q When did this chat take place?

A In 2007.

Q Did you pull other chats from uBuyWeRush's computer?

A Yes.
Q I'm going to show you what's been marked as Exhibit 16.3. Do you recognize this chat?
A Yes.
Q Is that in the same condition as when you found it on the computer you examined?
A Yes.
MR. BARBOSA: Government offers Exhibit 16.3 under the same exception.
MS. SCANLAN: Same objection, Your Honor.
THE COURT: Same ruling. Admitted.
(Exhibit 16.3 was admitted)
BY MR. BARBOSA
Q So the chat name we saw was "nCuX111."
Did this person provide further information about his nic?
A Yes.
Q What was it?
A Specifically, that his nic was "nCuX" from Skype, and then that he was using "nCuX111."
Q Were you aware of the nic "nCuX" in the carding community?
A Yes.
Q How were you aware of that nic?
A That it had been a carding nic prior to the appearance of track2 and bulba.
Q When had the nic "nCuX" stopped being a nic that you

were -- on the carding forums?
A Right when track2 and bulba became carding sites.
Q So were you able to follow up on that booookscafe e-mail account?
A Yes.
Q When was that?
A In February of 2011.
Q And had you seen that -- had you seen that booookscafe elsewhere in your investigation, before coming across it on the Caranza computer?
A Yes.
Q Where else?
A It was in the -- somebody using the HopOne server had logged into the booookscafe@yahoo e-mail account from the server.
Q So when you executed your search warrant on the booookscafe e-mail account, did Yahoo! also provide the same type of subscriber records and login records we've seen with the rubensamvelich account?
A Yes.
Q I'd like to show you what's been marked as Exhibit 5.1.
Do you recognize that?
A Yes.
Q How do you recognize that?
A This is the Yahoo! account management tool information

that was provided.
Q The subscriber records?
A Yes.
MR. BARBOSA: The government offers Exhibit 5.1.
MS. SCANLAN: Your Honor, if I may have one moment?
THE COURT: You may.
MS. SCANLAN: No objection to 5.1.
THE COURT: 5.1 is admitted.
(Exhibit 5.1 was admitted)
BY MR. BARBOSA
Q Looking at the first page of Exhibit 5.1, what was the username or login name provided?
A "Booookscafe."
Q And when was this account created?
A April 17, 2006.
Q And what was the full name that the user of the account had provided when subscribing for it?
A "Mr. dasdasdsa dadasdas."
Q What location information had been provided?
A New York, New York.
Q And birthday?
A October 11, 1971.
Q Did any of this information help further your investigation in terms of who was using it?
A No.

Q Do you rely on that type of information, typically?
A No.
Q Were you able to find out anything about this registration IP?
A It was a Russian IP address.
Q And would that have dated back to 2006?
A Yes.
Q Showing you now the login records, 5.2, do you recognize those?
A Yes.
Q How do you recognize that?
A Those -- the two blue IP addresses are HopOne IP addresses.

MR. BARBOSA: This is a two-page exhibit. Government offers Exhibit 5.2.

MS. SCANLAN: May I inquire?

THE COURT: Certainly.

VOIR DIRE EXAMINATION

BY MS. SCANLAN

Q Detective Dunn, this record -- I'm just not clear.
Did you get this from Yahoo!?
A Yes.
Q Just like this?
A Yes.

MS. SCANLAN: No objection.

THE COURT: 5.2 is admitted.

(Exhibit 5.2 was admitted)

DIRECT EXAMINATION

BY MR. BARBOSA

Q Let me clarify. The highlighting on the display exhibit, is that in the original?

A No. Yahoo! didn't highlight it. No, I'm sorry.

Q So the original exhibit is just black and white?

A Yes.

MR. BARBOSA: Is that what you were looking for?

MS. SCANLAN: No.

MR. BARBOSA: Just wanted to be sure. I'll publish this.

THE COURT: Counsel, just so we're clear, the offering was made with the coloration. The objection indicated that there was no objection to it coming in. There's clarification, so I didn't know if there's an objection to the coloring of the exhibit, since it didn't come from Yahoo! with the coloration.

MS. SCANLAN: And I apologize, Your Honor. I had thought that the exhibit was offered like the prior exhibits that were highlighted, where the actual exhibit was not going to be highlighted.

THE COURT: That's why I'm asking a clarification, if there's an objection or not, to the highlighted portions of

Exhibit 5.2.

MS. SCANLAN: There's an objection to it being highlighted as a substantive exhibit, but my understanding is that that will not be the case.

THE COURT: Is that correct, Counsel?

MR. BARBOSA: That's correct.

THE COURT: Okay. Then it's admitted.

MR. BARBOSA: All original exhibits in binders are not highlighted. These are only for display.

THE COURT: All right. Please continue.

BY MR. BARBOSA

Q We're looking at the login records for the booookscafe account on Exhibit 5.2.

When were the last logins that you found when you searched this account?

A The 21st -- the 7th of May, 2010. But from the HopOne, they were the 21st of April 2010.

Q Was that account being actively used at the time you finally searched it?

A No.

Q And you just referenced the HopOne server.

Are these the two that are highlighted in the middle?

A Yes.

Q Was that one of the HopOne servers you searched?

A Yes.

Q Is that where you found the booookscafe logins you had referenced earlier?
A Yes.
Q In general, what did you find in the content of the booookscafe e-mail account?
A I found pictures. I found e-mails. I found registration for domain names. I found online purchases records.
Q When you say you found domain registrations, were these domain registrations for the bulba or track2 sites?
A No.
Q What were they for?
A For sites related to nCuX.
Q Did you find registration -- server registrations for any servers related to your investigation?
A Yes. I found registration for the fvds server.
Q Did you find any instances of the usernames or passwords that you'd been looking for in your investigation?
A Yes.
Q Which ones?
A Shmak, smaus.
Q Did you find ochko?
A Yes.
Q When did this account -- based on your review of the login records and the content, when did it appear to have stopped being actively used?

A April/May of 2010.
Q Did you find any e-mails related to the identity of the account holder of the booookscafe account?
A Yes.
Q What types of e-mails?
A I found e-mails with his -- the name. I found e-mails sending things to other people, that were related.
Q Did you find receipts in the names?
A Yes.
Q Let's start with some of those. I'd like to show you what's been marked as Government's Exhibit 5.4 and 5.4A, the translation to that.
Do you recognize that?
A Yes.
Q Was that found in the booookscafe e-mail account?
A Yes.
MR. BARBOSA: Government offers Exhibit 5.4 and 5.4A.
THE COURT: 5.4A has been admitted, so it's only 5.4.
MR. BARBOSA: 5.4, then.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 5.4 was admitted)
BY MR. BARBOSA
Q What is this e-mail in 5.4 and 5.4A?
A This is the activation code for Roman Seleznev for the

website vkontakte.ru.
Q What is vkontakte.ru?
A It's a Russian-based social networking site.
Q Does it have any -- are there any similar sites in the United States?
A Facebook.
Q Who were these addressed to?
A Roman Seleznev.
Q Is this a multiple-page exhibit?
A So this is an e-mail to Roman Seleznev from Vkontakte. It says, "Roman Seleznev, Maks Kenzory wrote something on your wall. You can see the writing on your page."
Q And Page 3?
A "Roman Seleznev, Natalie Khmelina wanted to add you as a friend. You can confirm that you are friends or reject this request."
Q Why do these say to Roman Seleznev, as opposed to boookscafe, which was the e-mail address?
A Roman Seleznev was the name that was registered with Vkontakte.
Q So how does that display come through? Why doesn't it display as the boookscafe account?
A Because Vkontakte was sending the message to Roman Seleznev at the boookscafe e-mail account.
Q I'm going to move on to Exhibits 5.5 and 5.5A.

Do you recognize these?
A Yes.
Q This is both one page.
MR. BARBOSA: Government offers Exhibit 5.5 and 5.5A.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
Counsel, all the translations were admitted previously.
MR. BARBOSA: Okay. I will just offer the substance, then.
BY MR. BARBOSA
Q What is -- who is addressed in 5.5A?
A Roman Seleznev.
Q And what was this e-mail about?
A An order for a dictaphone.
Q Is this just a receipt?
A Yes.
Q Showing you now Exhibits 5.7, 5.7A, which has already been admitted, do you recognize those?
A Yes.
Q How do you recognize them?
A This is another order for Roman Seleznev.
MR. BARBOSA: Government offers Exhibit 5.7.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 5.7 was admitted)

BY MR. BARBOSA
Q What was this for?
A This was for an external microphone.
Q And was this -- who was this addressed to?
A Roman Seleznev.
Q And the e-mail address listed?
A "Boooks," with three "O's," "cafe@yahoo.com."
Q And the phone number that you found here, did this match up with anything else in your investigation?
A Yes.
Q What did it match up with?
A It's the phone number that I had seen in the rubensamvelich e-mail account.
Q Where else had you seen that?
A Western Union records.
Q And those Western Union records, did they have a name with them?
A Roman Seleznev.
Q Any other identifying information that was tied to that phone number?
A Passport, date of birth.
Q Okay. Had that phone number shown up in relation to the track2 site?
A Yes.
Q Where was that -- where had that phone number shown up in

relation to the track2 site?
A The domain registration.
Q Had it shown up in any of the DDoS?
A In the DDoS protection.
THE COURT: Counsel, before you move on to another exhibit, is this a convenient time to recess?
MR. BARBOSA: Yes, Your Honor.
THE COURT: We'll take our afternoon break.
(Jury exits the courtroom)
THE COURT: Counsel for the government, anything to take up?
MR. BARBOSA: No, Your Honor. Thank you.
THE COURT: Defense?
MR. BROWNE: No, Your Honor.
(Recess)
(Jury enters the courtroom)
THE COURT: Counsel, you may inquire.
MR. BARBOSA: Thank you, Your Honor.
BY MR. BARBOSA
Q I think we had just gone over Exhibit 5.7A and phone number -- where had you seen this phone number before?
A It was in the rubensamvelich e-mail account related to the DDoS protection services he was contacting.
Q Had that same phone number also shown up in the PayPal records?

A Yes.
Q I'm going to turn now to Exhibit 5.6.
Do you recognize that?
A Yes.
Q This is a six-page exhibit.
How do you recognize Exhibit 5.6?
A This is a receipt for a flower order that was in the booookscafe e-mail account.
MR. BARBOSA: Government offers Exhibit 5.6.
THE COURT: Any objection?
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 5.6 was admitted)
BY MR. BARBOSA
Q And 5.6A has already been admitted, so I'm bringing these both up on the screen in front of you.
Who are these flower order receipts addressed to?
A Roman Seleznev.
Q And what were the receipts for?
A This receipt was for an order of flowers to a Katya Berdnikova.
Q Do you know who Katya Berdnikova is?
A No.
Q What was the address they were ordered to be delivered to?
A Vladivostok, Russia.

Q Were there other flower order receipts in Exhibit 5.6A?
A Yes.
Q Turning to Page 3, who is this order for?
A This is an order for Svetlana Selezneva.
Q Is that highlighted, down towards the bottom of the page?
A Yes.
Q Was there a message included in the flower order for this one?
A Yes.
Q What was the message?
A "You are the most beautiful. But, no, Yevka (little Eve) is more beautiful, after all."
Q And what was the address this had been ordered to be delivered to?
A To Vladivostok, Russia.
Q Is that the same address -- that's not the same address from the passport; is it?
A No.
Q Have you seen that address before, though?
A Yes.
Q Is that the same address you saw in the internet store defencer receipt?
A Yes.
Q Were those both addressed to Roman Seleznev?
A Yes.

Q When were these both dated? Were these -- would you go over that?
A Yes. The defencer.ru order was dated September 19, 2009, and the flowers were July 11, 2009.
Q Turning to Page 5 of Exhibit 5.6A, who was this flower order for?
A Svetlana Selezneva.
Q And was that the same address in Vladivostok?
A Yes.
Q Now I'd like to turn your attention to Exhibit 5.3 and 5.3A.
Do you recognize these exhibits?
A Yes.
Q How do you recognize these?
A These are e-mails that were sent to boookscafe from the e-mail address ssav25@rambler.ru.
MR. BARBOSA: Government offers Exhibit 5.3.
THE COURT: Any objection?
MS. SCANLAN: I think I just saw the other version come up there.
Right there, is that part of the exhibit?
MR. BARBOSA: It is. I didn't believe that was part of the redactions. Sorry.
First page of 5.3A, is that what you're referring to?
MS. SCANLAN: Uh-huh.

THE COURT: So is there an objection?

MS. SCANLAN: Yes, Your Honor. I understood that to not be a part of this exhibit.

MR. BARBOSA: Did the Court intend that to be a part of the redactions?

THE COURT: That's correct, Counsel.

MR. BARBOSA: We'll redact it.

With that redaction, the government offers 5.3 and 5.3A again.

THE COURT: I take it there's no objection now, Counsel?

MS. SCANLAN: Correct, Your Honor.

THE COURT: It's admitted.

(Exhibits 5.3 and 5.3A were admitted)

BY MR. BARBOSA

Q What did you find attached to the e-mail in 5.3?

A Pictures.

Q Do you recognize anyone in these photos?

A Yes.

Q Who?

A The adult female is Svetlana Selezneva.

Q How do you recognize her?

A Because I've met her and interviewed her.

Q The "from" line for this e-mail coming from ssav25@rambler.ru, what is the name listed?

A "Svetlana."
Q Did you find any instances of the username "smaus" or the password "ochko" in the booookscafe account?
A Yes.
Q Can you take a look at Exhibit 5.8 and 5.8A? This is a five-page exhibit.
A I have 5.13 -- here we go.
Q Do you recognize those?
A Yes.
MR. BARBOSA: Government offers Exhibit 5.8.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 5.8 was admitted)
MR. BARBOSA: And 5.8A was already admitted?
THE COURT: Correct.
BY MR. BARBOSA
Q Turning your attention to these exhibits on the screen, why did you select these e-mails out of the account?
A Because they show a login name of "smaus," and some have an "ochko123" password.
Q So the first page, "smaus"?
A Yes.
Q What did the second page have?
A "Smaus" and "ochko123."
Q And the third page?

A "Smaus."
Q And you can look at them on the screen, if that's easier.
A Okay. Great.
Q The fourth page?
A "Smaus."
Q And the name that it was addressed to?
A Boris Grechkin.
Q Had you seen that name elsewhere?
A No.
Q Did you find any e-mails addressed to "seek," or nCux?
A Yes.
Q I'm showing you Exhibit 5.9 and 5.9A.
Do you recognize these?
A Yes.
Q And these are -- this is a long exhibit -- well, actually, no, this is one page. Sorry.
MR. BARBOSA: The government offers Exhibit 5.9.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 5.9 was admitted)
BY MR. BARBOSA
Q Where did the name "nCuX" show up here?
A "Dear nCuX."
Q And who was this from?
A Rupay Payment System.

Q When was that dated?
A December 6, 2006.
Q Was this early in the use of the account?
A Yes.
Q Did you find other e-mails addressed to nCuX later in the use of this account?
A Yes.
Q Let me show you what's been marked as 5.10 -- or related to nCuX -- 5.10A.
Do you recognize these e-mails?
A Yes.
Q This is ten pages.
What is the nature of the e-mails in 5.10?
A These are domain registrations related to domains associated with -- or containing the word "nCuX."
MR. BARBOSA: Government offers Exhibit 5.10.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 5.10 was admitted)
BY MR. BARBOSA
Q So using 5.10 as an example, what was this exhibit for? What was this e-mail for?
A This shows that on April 13, 2009, the domain nCuX.tv was successfully registered.
Q Were there receipts for other nCuX-related domains

included here?
A Yes.
Q Turning to Page 2, what was the domain there?
A NCuX.name.
Q Turning to Page 3, what was the domain name registration reflected there?
A NCuXlist.com.
Q Turning to Page 4, does it have several domains listed?
A Yes.
Q What were they, and when were they registered?
A NCuX.tv, nCuX.name, nCuX.asia, and nCuX.list.
Q Did any of these appear similar to the track2 or bulba domains you had been investigating?
A Yes.
Q Were you able to visit any of these sites?
A No.
Q Were they active, or had they been taken down by the time you began investigating?
A They were no longer active.
Q And the remainder of Exhibit 5.10 and 5.10A, are those just additional domain records for the same domains?
A Yes.
Q Turning your attention to the final page, 5.10A, when was that dated?
A May 23, 2010.

Q And what does this indicate?
A The deletion of the four domains I just listed.
Q So based on your review of these, what did that tell you about the use of these domains?
A That they were no longer being used.
Q Turning your attention to Exhibit 5.15, which is a 19-page exhibit, do you recognize this series of e-mails?
A Yes.
Q How do you recognize this series of e-mails?
A These are e-mails to the boookscafe e-mail account from people wanting to purchase cards.
Q Is this all -- all pages of 5.15, is this a continuous conversation with one person?
A Yes.
Q And does the owner of the boookscafe account participate in a conversation in this?
A Yes.
MR. BARBOSA: Government offers Exhibit 5.15, Your Honor.
MS. SCANLAN: No objection.
THE COURT: 5.15 is admitted.
(Exhibit 5.15 was admitted)
BY MR. BARBOSA
Q All right. We're going to go through this somewhat slowly.

Turning to Page 1 of Exhibit 5.15, have you gone over this conversation? Do you know the nature of this conversation?
A Yes.
Q What was it about?
A It was about the purchasing of credit card numbers.
Q Okay. How did the conversation begin, and what -- when was that?
A May 17, 2009, with an e-mail from rickcolho@yahoo.com.
Q What was the subject?
A "Dumps."
Q Based on your training and experience, what does "dumps" mean?
A Full credit card track information.
Q Can you read that in?
A "Hi. I want buy dump from you. I need to know. You send the balance? Track 1 and 2? For Liberty Reserve payment I can buy two pieces the first time? Please send me the prices for all country you have available. The only country I don't want is USA. I wait for your answer as soon as possible. Thank."
Q How did the booookscafe account holder respond?
A "Hi. No, I don't send balance, of course. I selling Europe Track 2 only. Can generate Track 1. For other rules, look on site nCuX.name."
Q Was that one of the domains that you found domain registration records for?

A Yes.
Q What happened next in this conversation?
A Rick Colho asked, "Hi. Do you have Liberty Reserve account?"
Q And again, what is a Liberty Reserve account?
A It was an online underground currency that people could use to transfer money.
Q Turning to Page 5, did there appear to be any response from booookscafe related to that?
A No.
Q What was the next message from Rick Colho?
A "Hi. I will transfer money to my WebMoney account, so will take two days. And after, I will place small order to start the business; okay? Can you send your BIN list? I see European others for 60 US. I want to know what is okay. I will place 200 US order for this time mix. Thanks for your attention."
Q What does the "BIN list" mean?
A The list of bank identification numbers that are currently available for sale.
Q Turning to Page 7, what did booookscafe respond?
A This is from Rick Colho again.
Q Oh, sorry. Turning to Page 9, what did the booookscafe account holder send to Rick Colho?
A "Hi. No, I accept only WebMoney. Also, my BIN list is EU

and Asia." And he provides four links from the nCuX.name site. And then for USA, he provides five links for those.

Q Did that include any with names that you recognized from elsewhere in your investigation?

A Yes. There was one nCuX.name/smaus BIN.

Q Did you find any e-mails sent from the boookscafe account containing BIN lists?

A Yes.

Q I'd like to take your attention to Exhibit 5.13.

Do you recognize that exhibit and the attachment?

A Yes.

Q How do you recognize that?

A This is a BIN list.

MR. BARBOSA: Government offers Exhibit 5.13.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 5.13 was admitted)

BY MR. BARBOSA

Q So turning to Exhibit 5.13, Page 1, what was the attachment listed?

A BinsZIP.txt.

Q And the subject?

A Sdaasd.

Q Undecipherable?

A Yes.

Q What was in the attachment? Were you able to review it?
A Yes.
Q Turning to Page 2, is that the beginning of the attachment?
A Yes.
Q What do we have here?
A So we have the BIN, which is the first six digits identifying the financial institution, followed by a dash, and then a number. That single-digit number indicates the number of cards that are for sale. And then the last is a description of who's the bank that owns that card, if it's known.
Q How many pages did this go through?
A Off the top of my head, I don't remember. It was a lot.
Q Scroll down to the bottom. Is that eight pages long?
A Yes.
Q I'll turn your attention to Exhibit 5.14, which is one page.
Do you recognize this exhibit?
A Yes.
Q How do you recognize this?
A This is an e-mail from boookscafe to Christopher Paar, Christof Paar.
Q Does it start with an e-mail from Christof Paar?
A Yes. No. It starts -- the top is an e-mail from boookscafe, but the beginning of the conversation is below,

yes.
Q So the first in the conversation is from boookscafe; is that correct?
A Yes.
MR. BARBOSA: Okay. The government offers Exhibit 5.14.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 5.14 was admitted)
BY MR. BARBOSA
Q So does this conversation begin at the bottom of the page?
A Yes.
Q And what did boookscafe write?
A "Dear Christof Paar: Is it DES or 3DES? Can I crack it with copacabana?" and then three examples.
Q Based on your training and experience, do you know what "DES" or "3DES" means?
A Yes. So "DES" is an encryption algorithm. It's an older encryption algorithm. And then "3DES," or triple DES, is a newer version of the DES encryption algorithm, which is much more difficult to break, if not impossible.
Q What is that encryption algorithm used for?
A It can be used for anything. It's commonly used with encrypted PIN numbers.
Q What is "copacabana"?

A It's a type of cracking software, hash cracking software.
Q What was Mr. Paar's response to boookscafe?
A "Unfortunately, there is no way of telling by looking at the ciphertext whether it is DES or 3DES. If it is DES, we can break it. There is no way to break 3DES for us (and most likely nobody else). One way of figuring out whether it is DES or 3DES is that you reverse engineer the software or hardware. Another way is that you send us one piece of plaintext and one piece of ciphertext. We can run copacabana on it. If we find the key, it is DES. And this check takes about one week. We have to charge Euro 250 up front for it. If we find the key, we'll charge another Euro 500. Regards, Christof Paar. PS, could you tell us what your application is? We need assurance that copacabana is not used for illegal purposes."
Q How did the boookscafe user respond?
A "I use it for illegal purpose. It's pinblocks of POS. Usually on POS 3DES, right? If you can help me with it, I can pay a lot of money. Thanks you."
Q What is a "pin block"?
A It's the encrypted PIN number that is entered on a PIN pad.
Q You mentioned you also found receipts related to the smaus server.
A Yes.
Q Can you take a look at Exhibits 5.1 -- or 5.11 and 5.11A?

And this is an 11-page exhibit.
A Okay.
Q Do you recognize those?
A Yes.
Q How do you recognize them?
A These are e-mails from firstvds.ru to booookscafe.
MR. BARBOSA: Government offers 5.11.
MS. SCANLAN: No objection.
THE COURT: It's admitted.
(Exhibit 5.11 was admitted)
MR. BARBOSA: 5.11A has already been admitted?
THE COURT: Correct.
BY MR. BARBOSA
Q I want to bring up just the English translation so it will be a little easier to read.
When was this dated?
A December 12, 2009.
Q And who was the addressee?
A Boris Grechkin.
Q And had you seen that name earlier, as we were going through the exhibits?
A One time.
Q And what was the subject of this e-mail?
A "First VDSHa product - Hosting Services VDS - Start #362611 (smaus.fvds.ru-188.120.225.60)-disk space added."

Q Do you recognize that IP address or domain name from your investigation?
A Yes.
Q Where had you seen that before?
A That's the IP address and domain from where the malicious software was downloaded onto the victim point-of-sale systems, and also one of the collection server IP addresses.
Q And is that on Exhibit 17.9, the infrastructure diagram?
A Yes.
Q Where is that at?
THE WITNESS: May I step down, Your Honor?
THE COURT: Yes, you may.
THE WITNESS: It's right here (indicating).
BY MR. BARBOSA
Q When you first came across that server, did it have that same domain name, starting with "smaus"?
A No.
Q What was the domain name you saw?
A "Shmak."
Q Is that why there's both "shmak" and "smaus" on it?
A That's correct.
Q How could an IP address have two different domain names?
A It just changed over time. The user decided to change it from "smaus" to "shmak."
Q So who would have the ability to change that domain name?

A The person who was leasing it.
Q The remainder of Exhibit 5.11, does that have additional receipts related to the smaus or shmak server?
A Yes.
Q And what were these related to?
A Exceeding the bandwidth that was supposed to be used, so overage notices.
Q Based on your training and experience, what did that tell you about the use of that server?
A That it was being used more heavily than it had been originally intended for, or spec'd out for.
Q Were there several resource overage notifications in this exhibit, in the booookscafe account?
A Yes.
Q And at one point, did they stop the user service?
A Yes.
Q I'm going to show you what's been marked as Government's Exhibit 5.17, and here's 5.17A.
Do you recognize this?
A Yes.
Q Was this in the booookscafe account, also?
A Yes.
Q Who was it addressed to?
A "To Roman."
MR. BARBOSA: Government offers Exhibit 5.17.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 5.17 was admitted)

BY MR. BARBOSA

Q What was the subject of this e-mail?

A "Happy Birthday Roman."

Q When was it dated, and what time stamp was on it?

A July 22, 2010, at 11:50 p.m.

Q What was Mr. Seleznev's birthday?

A July 23.

Q And do you know what time stamp was on this, based on your review of the Yahoo! records?

A It's Greenwich Mean Time.

Q What time would that have been in Vladivostok?

A 7:00 or 8:00 in the morning.

Q The following day?

A Yes, on the 23rd.

Q At some point, did you obtain a warrant for Mr. Seleznev's arrest?

A Yes.

Q When was that?

A In March of 2011.

Q Where did you believe Mr. Seleznev was located?

A In either Vladivostok, Russia, or Bali, Indonesia.

Q Did you request his extradition from Russia?

A No.
Q Why not?
A Because I didn't believe that the Russians would extradite a citizen. It's against their constitution.
Q Did you continue to monitor the bulbacc vending sites?
A Yes.
Q What did you observe on the bulba.cc vending site during the winter and spring of 2011?
A The winter of 2011 and the spring of 2011 was a very busy time for the sites. Specifically on April 12, 2011, there was an advertisement for the sale of a million credit card numbers.
Q If you could speak up?
A There was an advertisement for the sale of over a million credit card numbers.
Q You said during the winter and spring. Was there any point during that time period that business slowed down on the bulba website?
A Yes.
Q When was that, approximately?
A April 30, 2011.
Q Did you have any reason to believe -- did you learn any information about Mr. Seleznev's -- whether he had been injured around that time period?
A Yes.
Q How did you learn that?

A Through the news.
Q Did you attempt to determine whether the site was active around the time you believed he might have been injured?
A Yes.
Q How did you do that?
A I sent multiple messages to the support contact on the bulba site.
Q What kind of responses, if any, did you receive from the support on the bulba site?
A Just that I had to wait.
Q Can you take a look at Exhibits 2.10 through 2.15?
THE COURT: Through .15, Counsel?
MR. BARBOSA: Yes, 2.10 through 2.15.
MR. BROWNE: Sorry. What was the last one?
MR. BARBOSA: 2.10 through 2.15.
THE WITNESS: Okay.
BY MR. BARBOSA
Q Do you recognize each of those exhibits?
A Yes.
Q How do you recognize those?
A These are undercover conversations that I had with the admin who was responding to tickets on the bulba.cc website.
Q Do they all fairly and accurately represent the undercover communications you had with the admin at bulbacc?
A Yes.

MR. BARBOSA: The government offers Exhibits 2.10 through 2.15.

THE COURT: Any objection?

MS. SCANLAN: No objection.

THE COURT: They're all admitted.

(Exhibits 2.10 through 2.15 were admitted)

BY MR. BARBOSA

Q I'm going to start with Exhibit 2.13. When was this?

A May 4, 2011.

Q And who are the parties to this communication?

A Myself, using the nic "pcvcc2," and admin.

Q Why did you send this message?

A Because there had been no updated cards on the site, and I was also aware of the injury to Mr. Seleznev.

Q What was the response you received?

A That I needed to wait.

Q How long was it after you learned the defendant had been injured before the bulba site started posting fresh dumps again?

A Approximately two months, two-and-a-half months.

Q How long did the site continue to operate?

A Until very early January 2012.

Q During that down time, did you send additional messages to support?

A Yes.

Q Showing you Exhibit 2.14, is this another message you sent?
A Yes.
Q What did you say?
A "Need fresh tracks. When are they coming?"
Q Did you receive a response?
A Yes.
Q Is that on Page 2 of Exhibit 2.14?
A Yes.
Q What was the response you received?
A "Hi. Don't know when have. Need wait it."
Q Let me show you what's been marked as Exhibit 2.17.
Do you recognize this?
A Yes.
Q How do you recognize that?
A It's a screenshot I took of the bulbacc website.
Q That's just a one-page exhibit; is that right?
A Yes.

MR. BARBOSA: Government offers Exhibit 2.17.

MS. SCANLAN: No objection.

THE COURT: It's admitted.

(Exhibit 2.17 was admitted)

BY MR. BARBOSA
Q What are we looking at here?
A This is the announcement for the shop closing.

Q When was that?
A This was late -- the announcement came out late December 2011.
Q Could you read the announcement into the record?
A Yes. "Shop is closed. Shop is closed. Closed... Still open until 7 January 2012 totally. You must buy on remains balance or create ticket with your Liberty Reserve purse for refund. We closed because don't have more dumps. Good luck to all, and happy with new year. Contact only by contact support form. Our bases are sales, Track 2, 50 percent valid. A lot dumps, very cheap, $7 per one. Database 18, Track 2 only, 70 percent fresh. Database 19, Track 2 only, 99 percent fresh."
Q When you left the Seattle Police Department in 2013, what was the status of this case?
A The case remained open with an active warrant for Mr. Seleznev's arrest.

MR. BARBOSA: Just a moment, Your Honor.

THE COURT: Members of the jury, if you'd like to stretch at this time.

Ready, Counsel?

MR. BARBOSA: Yes, Your Honor.

THE COURT: Please be seated.

MR. BARBOSA: I have no further questions for this witness.

THE COURT: Cross examination?

MS. SCANLAN: Thank you, Your Honor.

If I may just have one moment to transfer systems here?

THE COURT: Sure. Members of the jury, if you'd like to stand and stretch again, please feel free to do so.

You can't accuse me of not giving you enough stretch time.

MR. BARBOSA: I'm going to remain seated, if you don't mind, Your Honor.

THE COURT: That's fine.

MS. SCANLAN: Your Honor, I apologize. We spent a lot of time making sure this works, and now it doesn't work.

THE COURT: That's fine.

Ready?

MS. SCANLAN: Yes. Thank you.

THE COURT: Cross examination? You may inquire.

CROSS EXAMINATION

BY MS. SCANLAN

Q Hello, again.

A Hi.

Q Let's talk about -- we're going to back way up to the beginning of your testimony and talk about general forensic practices when you seize a computer.

A Okay.

Q When you seize a PC or a laptop, do you generally determine whether it's on or off?

A Yes.
Q Why?
A If a computer is on and there's encryption running, you may be able to make a live image of it. If it's off, you'll keep it in that current state.
Q If you're not concerned about encryption, and a computer is on, what do you do?
A You would -- if there's an external battery that you can remove, or a way to power it off, you would power it off.
Q Why would you do that?
A To prevent any unnecessary writes to the hard drive.
Q And why are we preventing unnecessary writes to the hard drive?
A To maintain the device in the most pristine condition possible.
Q If you are worried about encryption -- and let's do this again.
What's encryption?
A Encryption is when the data is protected by a password or pass phrase that is required in order to unscramble the data; meaning without that password, it's not humanly readable or machine readable. It's just garbage.
Q And what relationship does that encryption process have to do with leaving it on or turning it off when you seize it?
A If the device is on and logged in, then you can run

forensic tools to extract the data in an unencrypted fashion.
Q And then what happens if it turns off?
A If you don't have the password, you're never going to get an image.
Q So this is when you do the stuff you're referring to as "live imaging"; right?
A Yes.
Q When you suspect there's encryption.
A Correct.
Q If you seize a computer, and it's on, and you suspect encryption, and then it -- you lose power, are you going to be able to turn it back on and image it?
A No.
Q Is that commonly known in the computer forensic field?
A Yes.
Q You indicated, previously, that when you do a live image, so when you don't turn it off first, that you do not use a write blocker; is that right?
A Correct.
Q And a write blocker is the thing that makes it so that your computer doesn't affect the drive when you're copying it; is that right?
A Correct.
Q You use, instead, a clean, sterilized drive; is that what you said?

A Yes.
Q Why do you do that?
A So that there's -- when you connect it to the computer that you're capturing the image from, there's nothing that could be written to the other drive. There's nothing present on your drive.
Q And why do you want to avoid having this intersection between your drive and the one that you're copying?
A You don't want to contaminate the drive that you're trying to -- that you're imaging.
Q What happens when you contaminate it, when the two come together? Does it make it harder to sort out what was there when you seized it?
A I guess, hypothetically, if you were to contaminate a drive?
Q Yeah.
A Yes, it would make it more difficult.
Q I'm not accusing you of contaminating a drive.
A We're hypothetically speaking about drive contamination.
Q Yes.
A Okay.
Q Let's talk about access dates.
A Okay.
MS. SCANLAN: And if I hit PC-1, can you put 1.1 up, please?

BY MS. SCANLAN

Q We're looking at Exhibit 1.1. Do you see this on your screen?

A Yes.

Q And this is actually an exhibit that you made about Schlotzky's; right?

A Yes.

Q And it has the last accessed date in the middle column?

A Yes.

Q And there was some questions, when you were talking to Mr. Barbosa, about the significance or insignificance of the last accessed date; do you remember that?

A Yes.

Q When we look here at this last accessed date, this is giving us information, right, about when the Schlotzky's server was connecting to these malware pieces?

A These malware pieces are on the Schlotzky's server. So this is when these pieces of software were being touched by the system in some way.

Q That's what I meant, except it makes more sense when you say it.

So that's what the access date thing is; right?

A Yes.

Q And you put that here on this exhibit?

A Yes.

Q Now, I know -- I think it was yesterday you testified about antivirus software and how it can affect access dates; do you remember that?
A Yes.
Q So antivirus software can change the access date on a file without me sitting down and messing with my computer; right?
A Yes.
Q Does antivirus software generally change a large number of access dates at the same time?
A It can, yes.
Q How common is it for it to change, for example, a hundred file dates and leave the other 500,000 file dates on a computer?
A It depends what kind of scan was run.
Q Well, just the auto scans.
A It's not uncommon for it to just scan -- to change maybe a thousand dates.
Q Okay. So we've been looking at Yahoo! accounts; right?
A Yes.
Q We've got the booookscafe and then the rubensamvelich.
A Yes.
Q And Yahoo! is a -- they provide free e-mail account services.
A Correct.
Q So if I had a Yahoo! account, how long would it take you

to hack into it, if you had all your stuff?
A I couldn't hack into it. Just -- if you had it, I mean, I would need to do -- I guess I couldn't hack into it.
Q You couldn't get into my Yahoo! e-mail address?
A With just the e-mail account? No. I mean, there are a myriad of techniques that could be used to hack into an e-mail account. But if I just had your Yahoo! e-mail account and access to the Yahoo! portal, no, I couldn't hack into it.
MR. BARBOSA: I'm going to object. Beyond the scope of direct, Your Honor. There was no discussion of hacking of e-mail accounts on direct.
THE COURT: That's sustained, Counsel.
BY MS. SCANLAN
Q Let's talk about bulba --
A Okay.
Q -- the bulba.cc.
You were just recently talking about this period of time when you came to understand that Mr. Seleznev had been a person who was injured in a bombing; right?
A Yes.
Q And that was in a cafe in Morocco?
A Marrakesh, yes.
Q What was your understanding, from all that information that you reviewed, of how long -- or how seriously Mr. Seleznev was injured?

A He was injured seriously enough to be medically evacuated to Moscow.
Q And the information that you had indicated that the doctors in Morocco thought he might die during the process of evacuation?
A Yes.
Q And how long did you understand his recovery period to be?
A Three to six months.
Q So he gets injured on April 20 of 2011; is that right?
A Yes.
Q And in May -- so April 28, and then the next month is May, right, of 2011 -- you are interacting with the bulba website; correct?
A Yes.
Q You were having these chats with support -- the person named "support."
A Yes.
Q And your understanding is that Mr. Seleznev, during that period, is down for the count, so to speak.
A He's -- yes.
Q And then on July 15 of 2011, there are 40,000 new tracks for sale on bulba; right?
A Yes.
Q So that's approximately two-and-a-half months after the bombing?

A Yes.
Q And on July 21, there's another 120,000 for sale?
A Yes.
Q And then when you were working with the Secret Service on this case, you have reports that come out sort of in this e-mail format to many of the other Secret Service offices; correct?
A Yes.
Q And they have reporting periods. So you'll send a report from you, in the Seattle office, to whomever you want to within the Secret Service, and it will have, in the header line, the reporting period that you're speaking of; correct?
A Yes.
Q So, for instance, August 25 of 2011 to December 11 of 2011 would be a reporting period.
A Yes.
Q And during that specific reporting period, so August 25 of 2011 -- so that's, what, almost five months after the bombing?
A Yes.
Q Through all the way to December of that year, there were no significant investigative steps taken on the bulba investigation; correct?
A Correct.
Q And that was because you believed that your primary suspect was injured?

A Yes.
Q And then there was another reporting period that kind of starts when the other one left off, so December 2011 to April 2012.
A Yes.
Q And there were no investigative steps taken then, or significant ones, because you believed your primary suspect was injured?
A Yes.
Q Now, you testified -- if you could look at Exhibit 4.11. Can you see that?
A No.
Q Okay. Now we see it; yes?
A Yes.
Q Okay. What are we looking at?
A The hosting information for bulba.cc and track2.name.
Q During your testimony regarding this exhibit, you explained something having to do with the anti-DDoS hosting site; correct?
A Yes.
Q And what is that again? What's an anti-DDoS hosting site?
A A site that provides distributed denial of service protection.
Q And what is distributed denial of service protection?
A It's to protect a site from a flood of traffic that would

otherwise prevent legitimate users from being able to access the site.

Q So denial of service attack, if you're going to attack a site, then you have -- you just sort of bombard it from all over, right, and then it can't function?

A There's a number of different tactics that can be used. That's one of them.

Q Go ahead. What are the tactics?

A So you can do what's called a Layer 7 attack, where you can ask the server on the other end to work really hard, which causes the back-end server to break. You can flood the actual internet pipes with so much traffic that they are unable to absorb it all, and have to drop traffic. You can attack the actual hardware switches so that they fail in a closed state. There's a number of ways, all involving sending malicious type of traffic.

Q And the bulba and the track2 websites had a lot of these types of attacks happen to them; correct?

A Yes.

Q So going back to this, you indicated that both bulba and track2, we don't know what the real IP address is, right, because of this anti-DOS [sic] hosting site?

A Correct.

Q But didn't you have information that they were hosted by an IP address belonging to ISPsharktag, in Las Vegas?

A I didn't have that.
Q You didn't have that information in October of 2013?
A I was not with law enforcement October 2013.
Q So that was after you left.
A Yes.
Q So I guess you probably don't know whether anyone followed up on that.
A That's probably a good guess.
Q Okay. Let's talk about rubensamvelich; okay?
A Okay.
Q Is it "samvelich"?
A I always called it rubensamvelich. I don't know -- that's just how I pronounced it.
Q Okay. But we can understand each other. Because I'm probably going to say it the other way.
You understand what I'm talking about?
A Yes.
Q Okay. So can you look at your screen, what's been marked as Defense Exhibit 108?
A Yes.
THE COURT: Counsel, do you have copies for the Court?
MS. SCANLAN: Yes.
MR. BROWNE: Your Honor, may I approach?
THE COURT: Yes. Thank you, Counsel.

THE CLERK: Defendant's Exhibit 108 is marked.

MS. SCANLAN: I apologize, Your Honor.

THE COURT: Ready?

MS. SCANLAN: Yes. I'm going to make this work.

BY MS. SCANLAN

Q Do you see Page 1 of this?

A Yes.

Q Do you see Page 2?

A Yes.

Q Do you recognize this?

A Yes.

Q What is it?

A It's a counterfeit letter from the Australian Federal Police to antiddos.org.

Q And where did you locate this?

A It was in the rubensamvelich e-mail account.

Q Does it look the same as it did when you found it in the account?

A Yes.

MS. SCANLAN: The defense moves to admit Exhibit 108.

MR. BARBOSA: No objection.

THE COURT: 108 is admitted.

(Exhibit 108 was admitted)

MS. SCANLAN: Permission to publish?

THE COURT: Granted.

BY MS. SCANLAN

Q How is that looking on your screen? Can you see it?

A Yeah.

Q Okay. What is this? What's this first page we're looking at?

A So this is an e-mail thread that begins with an e-mail from Arian, A-R-I-A-N, @yahoo.com to info@antiddos.org. It says, "Hello. Thank you for your report. I ask you to scan a copy of this letter on your letterhead with your seal of your organization. We immediately take measures to stop the infringing works sites."

There's one from -- I'm sorry. That was from antiddos to Arian. The one above that is from Arian to antiddos. It says, "Attached legal document regarding official statement of intent criminal proceedings against domain track2.tv hosted by antiddos.org. Please find the requested document pursuant to your official inquiry of 2/25/10. This is an official certified document. We appreciate your immediate confirmation receipt of this correspondence. Regards, Dr. Arian A." And then that thread is later then forwarded to rubensamvelich@yahoo.com.

Q Okay. So the antiddos is the hosting site?

A Yes.

Q And they're communicating with the rubensamvelich e-mail account holder regarding this information?

A Yes.
Q And if we look at Page 2, this is a letter that has on the top of it "Australian Federal Police"; correct?
A Correct.
Q It says, "Advanced Research Department for Intelligence Against Financial Data Theft."
A Yes.
Q And essentially, what it says in here is that this website is stealing financial information, and so the hosting site should shut it down?
A Correct.
Q And you -- so you found this on the rubensamvelich e-mail account; right?
A Yes.
Q But this is not real?
A Correct.
Q So -- and how do you know it's not real?
A Because I contacted the Secret Service in Sydney, Australia, and they verified that the Australian Federal Police don't have an Advanced Research Department for Intelligence Against Financial Data Theft; that Dr. Arian Ards is not an employee, and they don't even have the rank of colonel, for Mark Hopper, who's not an employee either.
Q So somebody who's not the Australian Federal Police sent this letter to the host of the track2 website?

A Yes.
Q Okay. Let's talk about PayPal records. You talked about that; right?
A Yeah.
Q So you testified about the PayPal records that you found in the rubensamvelich account that were -- for the name "Roman Seleznev."
A Yes.
Q But you found -- and then you testified that PayPal records often carry more validity than other records, because they have all these verification steps; right?
A Correct.
Q And what are the PayPal verification methods again?
A I don't know all of the verification methods that they use on the back end, but they're subject to more stringent financial regulations. So I don't know -- from an address verification, name verification, ID verification, I don't know what exact steps they follow. But they are subject to more stringent rules.
Q So in addition to the Roman Seleznev PayPal records that you found on the rubensamvelich e-mail, you also found PayPal records for Roman Ivanov; correct?
A Yes.
Q In fact, you found one PayPal account for Roman Seleznev; correct?

A Yes.
Q And three PayPal accounts for Roman Ivanov?
A I'd have to look at the records. If you have them, I can review them.
Q Can you see that?
A Yes.
MS. SCANLAN: And, Your Honor, I have copies.
THE CLERK: Defendant's Exhibit 109 is marked.
BY MS. SCANLAN
Q Do you see this Page 1 of 2 and 2 of 2?
A Yes.
Q And then 1 of 2 and 2 of 2 here?
A Yes.
Q And then again?
A Yes.
Q Are these the PayPal records that you pulled off Rubensamvelich's e-mail account, the Yahoo! account?
A I don't know if these are from that, or if we got these from -- these may have been records directly from PayPal.
Q You're right. You're right. I apologize. These are records that are directly from PayPal.
Do they look the same as when you got them?
A Yes.
MS. SCANLAN: The defense moves to admit Exhibit 109.
MR. BARBOSA: No objection, Your Honor.

THE COURT: 109 is admitted.

MS. SCANLAN: Permission to publish?

THE COURT: Granted.

(Exhibit 109 was admitted)

BY MS. SCANLAN

Q Okay. So what are we looking at here?

A PayPal account info for Roman Ivanov.

Q Do you see that part I just brought up?

A "Personal - Unregistered - Russian Duplicate (Russia)."

Q Can you see this?

A Yes.

Q So this is Roman Ivanov at the rubensamvelich e-mail address; correct?

A Yes.

Q Do you see here there's an address listed?

A Yes.

Q In Russia?

A Correct.

Q And there's a phone number given for Roman Ivanov; correct?

A Yes.

Q Okay. And then this is the second of the three PayPal accounts; correct?

A Yes.

Q So we have the e-mail address, and then we have a phone

number and an address in Moscow.
A Correct.
Q Okay. And then the third account, same deal. We have information about the -- who this person is, the e-mail address, and the phone number.
A Correct.
Q So you also looked at NuSphere records.
Do you remember talking about that?
A Yes.
Q Can we pull up Exhibit 15.14, please?
THE COURT: 14.15 or 15.14?
MS. SCANLAN: 15.14.
Can you highlight this bottom portion right here? Thank you.
BY MS. SCANLAN
Q Okay. Do you see this?
A Yes.
Q So what were the NuSphere records, again?
A They were a DDoS protection service.
Q Okay. So this is another one of these things that prevents or helps you when you have one of the attacks on your site?
A Correct.
Q And they're addressing their customer as Roman Ivanov?
A Yes.

Q And then Exhibit 6.5, this is an e-mail that you found in the rubensamvelich account?
A Yes.
Q And this e-mail is addressed to Roman Ivanov?
A I see, "Roman." I'm looking for "Roman Ivanov" in here. I see, "Hi, Roman." I'm -- you'll have to point out where the "Ivanov" is, because I don't see it.
Q That may be because I have the wrong number. I think you're right.
Okay. How about 15.2? So this is all these Western Union records; correct?
A Yes.
Q And this -- if we look on the left-hand side of this and we pull up the payee name --
A Yes.
Q This goes on -- there's lots of pages of this; right?
A Correct.
Q And a whole bunch of these Western Union records, when you were looking at these names, they're all for Roman Ivanov; right?
A Yes.
Q Thank you.
Okay. So let's talk about the malware, in general. We've been referring to it as the kameo malware.
You could download -- you just went out and you downloaded

the malware; right?
A Correct.
Q To the internet -- the shmak internet site?
A Yes.
Q Did you need a password?
A No.
Q Username?
A No.
Q You downloaded shmak.exe?
A Yep.
Q And shmak2.exe?
A Yep.
Q Dc2.exe?
A Dtc2.exe.
Q Yes. Zameo.exe?
A Yes.
Q And dtc4.exe?
A Correct.
Q And you were able to take the downloads that you just went and got off the internet and look at that malware, as it functioned; correct?
A Yes.
Q Let's talk about -- generally about the businesses that were subject to these malware attacks.
You testified earlier that the antivirus programs that

were available at the time of the Schlotzky's Deli intrusion would not have kept kameo out; right?

A That's correct.

Q But Schlotzky's Deli was not payment-card-industry compliant; is that right?

A I don't know what their PCI status at the time was.

Q Well, when the forensic investigations were done, they were not PCI compliant in terms of having the protections that were required by the PCI system.

MR. BARBOSA: Objection. He just answered that he didn't know.

THE COURT: Let's hear -- he's heard the entire question now, then you can object again, Counsel.

You have heard now the entire question. Your answer?

THE WITNESS: Can she repeat the last question one more time, sir?

THE COURT: Yes.

BY MS. SCANLAN

Q You know what might be easier? I can switch businesses, because it's the same for each one.

A Okay.

Q So Broadway Grill?

A Yes.

Q They had that text file, right, with 32,000?

A Correct.

Q The fact that that text file exists is not compliant with the payment card industry standards; correct?
A As I know them, yes.
Q Well, you testified about them earlier; right?
A Yes.
Q In fact, every single one of these businesses, in some manner or another, was not up to par with the payment card industry standards, in terms of their protections?
A I did not do a PCI audit on every single business, so I can't answer that question.
Q You reviewed all the private forensic audits; right?
A Yes.
Q You didn't get that information from there?
A I just don't remember it --

MR. BARBOSA: Objection. Hearsay.

THE COURT: It's overruled.

BY MS. SCANLAN
Q Let's talk about the Firefly connection to all of this.

So the Firefly is a division -- or a subsidiary of Granbury; right?
A I believe it's one of their product lines.
Q Okay. They're connected.
A Yes.
Q And Firefly provides support services to small businesses, pizza restaurants, that kind of thing?

A Correct.
Q They're supporting the point-of-sale systems; correct?
A Yes.
Q So they -- you install a point-of-sale system. And then you're in the middle of a rush, and your computer goes down.
You call them, they log in remotely, and help you fix it?
A Yes.
Q So they log in remotely through one of these remote desktop portals?
A Yes.
Q And so Firefly, or Granbury, they had the same password to be used to do these logins for lots of these businesses; right?
A Correct.
Q So once somebody, a hacker, multiple hackers, figured out what that password is, you can get into all these businesses?
A Yes.
Q So those businesses that had these Firefly generic passwords, they're vulnerable to attacks from all different sources; right?
A That have that username and password, yes.
Q So people who can run the port scanning?
A It's not just the port scanning. You'd also need to know the username and password.
Q But the people who got ahold of that information, they can get into all these businesses?

A Yes.

MS. SCANLAN: Your Honor may have -- oh, no.

BY MS. SCANLAN

Q Broadway Grill?

A Yes.

Q You talked about that -- we were just talking about that file with the 32,000 credit card numbers; right?

A Yes.

Q And that that was zipped up, so made smaller.

A Yes.

Q And it was sent to sendspace.

A Yes.

Q That's the only business where the credit card numbers were sent to spendspace; right?

A Correct.

Q So beyond that, the sendspace -- whoever is on the other end of the sendspace, you can't identify any other connection between sendspace and the taking of the credit cards from these businesses?

A Yeah. None of the other businesses had that big file present.

Q So once it's sent to sendspace, just so I'm clear, you can't say it went to sendspace, and then it went to one of these servers; correct?

A Correct.

MS. SCANLAN: Your Honor, may I have one moment?

THE COURT: You certainly may.

MS. SCANLAN: Thank you.

Nothing further.

THE COURT: Redirect?

MR. BARBOSA: Thank you, Your Honor.

REDIRECT EXAMINATION

BY MR. BARBOSA

Q Ms. Scanlan asked you a number of questions about forensic examinations, and you discussed encryption.

If you are concerned about encryption, why would you leave the computer on?

A So that you can access it and create a live image.

Q And how does that help you deal with the potential problem of encryption?

A The encryption is typically done at the disk level. And so if you're able to access the computer at the operating system or application level, you can make an unencrypted image of the operating system partition.

Q Okay. So what type of cases are you typically concerned about encryption on a suspect's computer?

A On hacking cases.

Q Is this a hacking case?

A Yes.

Q Were you concerned that the defendant's computer might be

encrypted?
A Yes.
Q How concerned were you that his computer might be encrypted?
A Very concerned.
Q What would have happened if his computer had been encrypted and you had not been able to make a live image?
A We would not have been able to capture any of the data in a useable format.
Q So if you seize a computer that you believe may be encrypted, and it's turned on, would you have left it on?
A Yes.
Q What about if the computer -- if you weren't able to obtain a search warrant right away, and that computer runs down its power, would you attempt, in any instance, to try and apply power to it?
A Yes.
Q Why?
A To keep it from running out of battery and encrypting itself.
Q What if it appeared dead? What if you were concerned that it had encryption, but it already appeared dead? Would you do that for any reason? Would you use a last-ditch effort?
A I'd probably just leave it alone.
Q Would you ever plug it into power, though?

A Sure.
Q What reasons might you plug it into power?
A If I thought that there was still power to the drive, if the computer drive was still on.
Q Do some computers, after running down power, do they go into sleep modes or deeper hibernation states?
A Yes.
Q Can you tell whether they're in a sleep mode or deeper hibernation state without repowering them?
A No.
MS. SCANLAN: Objection. This is outside the scope of cross.
THE COURT: It is starting to go a little bit afield, Counsel. Sustained.
BY MR. BARBOSA
Q Let's talk about the last accessed dates that Ms. Scanlan went over with you. She was looking at Exhibit 1.1 with you.
And reference the last accessed dates for the malware on the Schlotzky's Deli system, you -- I believe you said that those indicate when the system had touched the program?
A Yeah.
Q Okay.
A I mean, I have an opinion about these.
Q What is your opinion about those?
A I believe that the hacker came back in on 4/15 to fix

something.
Q Can the last access dates be affected by the system alone?
A Yes.
Q Okay. What type of system processes can affect a last accessed date?
A Specifically, the antivirus application running on the system. There can be -- restore points can change access date times. There's a number of different processes that can change those.
Q Can operating system update attempts, or program updates, occur?
A Yes.
Q You mentioned that this can affect a number of files on a system as a computer is going about its business.

How many potential files could be affected by antivirus or other programs?
A A few to a few thousand.
Q Ms. Scanlan also discussed the bombing incident in Morocco and Mr. Seleznev's injury, and the fact that you received responses to your inquiries.

Who -- what was the person on the bulba site who was responding to you? What was the title they were using?
A I believe it was "admin."
Q Okay. Did you also receive responses from "support"?
A Yes.

Q Is there a difference between "admin" and "support"?
A Yes.
Q Did you see any evidence in any of the accounts, the e-mail accounts, that the bulba administrator had additional people helping him? Just a moment.
A I don't believe in bulba. They were in rubensamvelich.
Q Turning your attention to 6.13, this is an e-mail with Black Lotus.
Did the operator of the track2 site indicate anything about having other support?
A Yes.
Q What did he say?
A "I have high-skilled administrator. He on ICQ. I can give you his ICQ to speak."
Q Let's talk about the PayPal records you found for Roman Ivanov.
MS. SCANLAN: I think you're on my computer screen.
MR. BARBOSA: I think I am.
BY MR. BARBOSA
Q This is from Defense Exhibit 109.
Do you see the phone number that was listed on the PayPal records for the Roman Ivanov named account?
A Yes.
Q Is it the same on each one?
A Yes.

Q Is that the same 5285 number that you'd seen in the account using the name Roman Seleznev?
A Yes.
Q You testified that you researched both the "Roman Ivanov" and the "Roman Seleznev" name, and were looking for commonalities or links.
What did you mean by looking for commonalities or links?
A I was looking for anything related to either of those two names that linked back to the overall investigation.
Q What type of connections were you looking for in these columns with any of the names that you'd come across?
A I was looking for phone numbers, geographic locations that matched up with the IP addresses that we had, birth dates.
Q Okay. Did you find anything that linked up between the Roman Ivanov -- the many, many pages of Roman Ivanov names in these records and other information, such as a phone number, date of birth, or passport number, elsewhere in your investigation?
A No, I did not.
Q Turning your attention to 15.2A, did you find anything that linked up with the name "Roman Seleznev"?
A Yes, I did.
Q What was it?
A The phone number.
Q Was that the same phone number that was on all four of the

PayPal accounts?
A Yes.
Q And in this record from Western Union, did this link up with any other identifying information?
A With his passport number.
Q Where else had you seen that passport number?
A In his passport, as well as in the HopOne server flight records.
Q Did it also link up with the same date of birth?
A Yes.
Q And for the Roman Seleznev PayPal account, was there any other identifying information, such as an address, that linked up with other parts of your investigation?
A Yes.
Q Where have you seen that address, the Ostryakova address?
A On the shipping -- or on a number of different places, including his passport.
Q Did you see that in the nCuX chat with Cesar Caranza?
A Yes.
Q What about in his orders for other items in the boookscafe account?
A Yes.
Q Let's talk about the malware server a little bit, the shmak/smaus server in Russia. You said you navigated to that site.

How did you know the address for that site?
A Because I had seen it in the typed URLs for the downloading of the malware to the victim servers.
Q Was that site -- could you Google that site and find its address?
A No.
Q Based on your training and experience, how would you find the address for that site?
A You would have to know it was there through an investigation.
Q So could any hacker have just navigated to that site?
A They could have. Anybody could have navigated there, yes.
Q What would they have needed to know?
A They would have needed to know the exact IP address, as well as the name of the file they wanted to download.
Q And in your training and experience, would multiple independent hackers send their stolen credit card numbers to the same computer server?
A No.
Q Why not?
A Because they don't control those servers, so they're giving their stolen numbers away.
Q Is there value to those stolen numbers?
A Yes.
Q What's the value to those stolen numbers?

A For a fresh card number, anywhere from $20 to $50.

MR. BARBOSA: Your Honor, I have no further questions.

THE COURT: Further cross?

RE-CROSS EXAMINATION

BY MS. SCANLAN

Q Another source of the IP address for malware could be in these chats in a carding forum; correct?

A Could have been.

MS. SCANLAN: I have nothing further.

THE COURT: Anything further from the government?

REDIRECT EXAMINATION

BY MR. BARBOSA

Q Just one question. Why would somebody publicly list their IP address for where they stored their malware, in a carding forum?

MS. SCANLAN: Objection. Calls for speculation.

THE COURT: What's this based on, Counsel?

MR. BARBOSA: Based on your training and experience in carding investigations, which I believe he's established himself.

THE COURT: It's overruled on those grounds.

THE WITNESS: There is no reason somebody would do that.

MR. BARBOSA: Thank you. No further questions.

THE COURT: Any objection to this witness being excused, by the government? Counsel?

MR. BARBOSA: No, Your Honor. Thank you.

THE COURT: Any objection to this witness being excused, by the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Thank you, sir. You're excused.

THE WITNESS: Thank you, Your Honor.

THE COURT: Members of the jury, we have come to the close of today's trial. Thank you for being present, and thank you for being jurors. We'll see you all tomorrow morning with a new witness, ready to go at 9:00 a.m. Have a good evening.

(Jury exits the courtroom)

THE COURT: Anything to take up, counsel for the government?

MR. BARBOSA: No. Thank you, Your Honor.

THE COURT: Counsel for the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Thank you. Have a good evening.

(Adjourned)

(End of requested transcript)

* * *

I certify that the foregoing is a correct transcript from the record of proceedings in the above matter.

Date: 8/17/16 /s/ Andrea Ramirez

Signature of Court Reporter